CASA DI RIPOSO
CARTIGLIANO

Allegato al
PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI
Misure di sicurezza e analisi del rischio

approvato con deliberazione del C.d.a. n. 18 del 18/09/2020

CASA DI RIPOSO CARTIGLIANO

CASA DI RIPOSO CARTIGLIANO

PIANO PER LA SICUREZZA DEI DATI

(digitali e su supporto durevole)

Aspetti generali

Il documento descrive il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici secondo buone prassi di comportamento degli addetti e dell'organizzazione.

Il documento è redatto in conformità al decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, il piano integra le modificazioni apportate con l'entrata in vigore del Reg. UE 2016/679, alle linee guida in materia di dossier sanitario, allegato A alla deliberazione del Garante del 04/06/2015, al provvedimento del Garante del 7 marzo 2019 "disciplina di protezione dei dati in ambito sanitario" e alle misure adeguate di sicurezza ICT.

Il documento illustra le misure di sicurezza relative al processo di gestione, dei documenti informatici e non, del sistema informatico e informativo dell'ente.

In sintesi, partendo dall'analisi dei rischi, il Piano descrive le misure da adottate per garantire l'efficacia della sicurezza dei dati/documenti intesa come riservatezza (autorizzazione all'accesso), disponibilità ed integrità (protezione da incidenti o usi impropri).

Si intende per rischio, la probabilità e la gravità di un eventuale danno alle libertà della persona interessata ovvero al proprietario dei dati.

Entrata in vigore e campo di applicazione

Il nuovo regolamento entrerà in vigore il _____. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento, oltre ad essere pubblicato nella intranet dell'Ente e nel sito istituzionale, verrà consegnato a ciascun dipendente che dovrà sottoscriverlo al momento dell'instaurazione del rapporto contrattuale o al momento della richiesta delle credenziali di autenticazione per l'accesso ai vari strumenti informatici.

Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, specializzando, consulente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

I reati informatici

Appare conveniente suddividere in macro-categorie le aree di intervento:

Frodi informatiche;

Falsificazioni;

Integrità dei dati e dei sistemi informatici;

Riservatezza dei dati e delle comunicazioni informatiche.

La macro-categoria delle frodi informatiche è regolamentata dall'art. 640-ter del Codice Penale, contenuto all'interno del Titolo XIII "dei delitti contro il patrimonio", Capo II "dei delitti contro il patrimonio mediante frode", e recita così: art. 640-ter ("Frode informatica"): "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito.."

Si parla qui di un reato consistente nel trarre in inganno un elaboratore elettronico, al fine di ricavarne un guadagno economico (per sé o per altri complici), a danno di un soggetto terzo (solitamente il detentore dell'elaboratore elettronico).

Si tratta perciò di un'estensione del reato di truffa descritto all'art. 640 c.p. "Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé e ad altri un ingiusto profitto con altrui danno, è punito.."

Tra i reati che più frequentemente vengono compiuti, e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le cd. pratiche di Phishing e quelle di diffusione di appositi programmi truffaldini, definiti Dialer.

Il phishing altro non è che un'attività finalizzata ad estorcere dati personali (in prevalenza legati alle carte di credito od ai conti bancari) attraverso una richiesta esplicita al suo legittimo possessore. Il principale metodo per porre in essere il phishing è quello di inviare una mail in tutto e per tutto simile a quella che verrebbe inviata da un regolare istituto (banca, provider, ecc. e con relativo logo identificativo), nella quale si riportano vari tipi di problemi tecnici (aggiornamento software, scadenza account, ecc.) che motivano l'utente a cliccare sul link riportato nella mail per andare ad aggiornare i propri dati personali.

Chiaramente il link non porta al "vero" sito dell'istituzione, ma ad un sito fasullo ed opportunamente creato dall'autore del reato di phishing, che si impossesserà così dei dati inseriti dall'utente.

Dal punto di vista della prevenzione il phishing si configura come uno di quei reati che possono facilmente essere debellati con una corretta informazione agli utenti.

A tal scopo una lista di punti chiave nella prevenzione del phishing:

• Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti ad esempio chiavi di accesso al servizio di home banking o altre informazioni personali;

• è possibile riconoscere le truffe via e-mail con qualche piccola attenzione: generalmente queste e-mail non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati; fanno uso di toni intimidatori; non riportano una data di scadenza per l'invio delle informazioni;

• nel caso in cui riceviate una e-mail contenente richieste di questo tipo, non rispondete alle e-mail stessa, ma informate subito il titolare;

• non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale;

• diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;

• quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con “https://” e non con “http://” e nella parte in basso a destra della pagina è presente un lucchetto;

• diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso;

• Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo.

Un altro tipo di reato che rientra nella categoria delle “frodi informatiche” è l’uso del cosiddetto Dialer.

Il dialer è un piccolo programma (pochi kilobyte) appositamente scritto per dirottare la connessione Internet dell’ignaro utente verso un altro numero telefonico, spesso di tariffazione internazionale e comunque sempre molto più caro rispetto alla comune chiamata telefonica al numero POP del proprio provider.

Attraverso l’utilizzo del dialer il guadagno è multiplo; operatori di telefonia, società produttrici dei dialer, webmaster.

E’ però da precisare che l’utente finale (singolo o ente che sia) viene colpito dal dialer solo nel momento in cui effettivamente lo scarica e lo installa sul proprio computer. Il dialer infatti è un normalissimo programma e come tale deve preventivamente essere installato per poter essere eseguito.

Una volta installato sarà il dialer che automaticamente sostituirà il numero ordinario di connessione con un numero a tariffazione maggiorata.

Anche per la frode mezzo dialer, come per il phishing, molto importante è l’informazione dell’utenza Internet, la quale può proteggersi da questa truffa attraverso pochi e semplici accorgimenti.

Innanzitutto è possibile disabilitare presso il proprio operatore telefonico le chiamate verso numerazioni internazionali e/o verso i numeri speciali a pagamento. In secondo luogo è possibile installare appositi software (definiti “stop dialer”) in grado di avvisare l’utente quando un programma terzo tenta di dirottare la connessione verso un altro numero telefonico non previsto. Altro provvedimento che è possibile adottare è quello di utilizzare una linea telefonica basata su tecnologia xDSL od a fibra ottica che, effettuando chiamate dirette e verso un solo numero, non subisce alcun danno dai dialer.

La seconda macro-categoria, quella delle falsificazioni, è regolamentata dal Codice Penale attraverso l’art. 491-bis contenuto nel Titolo VII “dei delitti contro la fede pubblica”, Capo III “della falsità in atti”: “Se alcuna delle falsità

previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli."

Il problema principale è che il documento informatico non viene compreso nella sua vera essenza che lo slega dalla materialità; mentre il documento cartaceo lega indissolubilmente contenuto e contenente, nel documento informatico tutto ciò non avviene ed è dunque limitativo ricondurlo al "supporto informatico".

Detto ciò bisogna quindi chiarire cosa si intende per "documento informatico": Il documento informatico è sostanzialmente un documento immateriale e dinamico, ed è la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" in quanto non vi è alcuna distinzione tra l'originale e la copia. Non si tratta dunque di un mero cambio di supporto rispetto al preesistente documento cartaceo, ma di un cambio nella concezione vera e propria di documento che nell'informatica, come detto, assume i caratteri di rappresentazione.

Il Codice Penale regolamenta poi una terza macro-categoria, che riguarda l'integrità dei dati e dei sistemi informatici, attraverso vari articoli, tra cui il 635-bis sul "danneggiamento di sistemi informatici e telematici", contenuto nel Titolo XIII "dei delitti contro il patrimonio", Capo I " dei delitti contro il patrimonio mediante violenza alle cose o alle persone"; "Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con.. se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione ..."

L'art. 635-bis del Codice Penale ripropone il reato di danneggiamento (previsto dall'art. 635 c.p.) in rapporto non solo alle apparecchiature informatiche o telematiche, ma anche ai dati, informazioni o programmi in esse contenute, necessariamente caratterizzati da immaterialità e difficili da punire con il generico reato di danneggiamento.

Nell'ambito dell'art. 635-bis si parla infatti di danneggiamento totale o parziale, di deterioramento e di distruzione. Con la prima espressione si fa riferimento alle modalità attraverso cui si può rendere del tutto o in parte inservibile un sistema informatico/telematico, con la seconda ci si riferisce alla creazione di guasti in grado di far scemare le prestazioni del sistema, mentre nella terza espressione ci si riferisce ad un'azione di annullamento totale di un sistema.

La miglior tecnica preventiva adottabile dall'utenza (privata o ente) è quella di dotarsi di efficienti sistemi di backup, in grado di sopperire all'eventuale perdita di dati e informazioni.

Aggravante del reato "danneggiamento di sistemi informatici e telematici" è l'art. 420 c.p. "attentato a impianti di pubblica utilità" contenuto nel Titolo V "dei delitti contro l'ordine pubblico";

Il Codice Penale interviene anche estendendo l'art. 392 ai sistemi informatici (comma 3); "Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito a querela della persona offesa, con ……...

Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o

cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico."

A tal riguardo viene punito colui che ricorre al "regolamento di conti" attraverso l'uso della violenza sulle cose al fine di manifestare un preteso diritto.

Riferito all'informatica si tratta dell'alterazione, modifica o cancellazione in tutto od in parte di un programma al fine di turbarne il corretto funzionamento.

Interessante da analizzare è infine l'art. 615-quinquies, attraverso cui si meglio precisa un aspetto già genericamente affrontato dall'art. 635-bis. Contenuto nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio", recita: art. 615-quinquies ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"): "Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito..

Con l'art. 615-quinquies si mira a reprimere la "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico", tutti i programmi cioè rientranti sotto la categoria di malicious software (o malware).

Il fatto che vi sia un articolo del Codice Penale unicamente dedicato a questa tipologia di software, evidenzia come la diffusione stessa di questi malware sia molto alta. Le categorie che rientrano sotto l'etichetta di malware sono molte ma, in linea generale, sono tutte accomunate dal medesimo scopo di danneggiare un sistema informatico (specialmente in riferimento alla sua parte "software").

La categoria di malware più diffusa e conosciuta è quella dei virus, speciali parti di codice che si diffondono copiandosi all'interno di altri programmi, in modo tale da essere eseguiti ogni volta che il file infetto viene aperto.

La diffusione dei virus è legata alla trasmissione di questi file infetti, che può avvenire sia attraverso comuni supporti di memorizzazione magneto-ottica, sia attraverso una distribuzione su reti telematiche. Queste ultime, in special modo Internet, hanno poi dato terreno fertile alla diffusione di altri malicious code, tra cui worm, trojan horse, backdoor e spyware, solo per citare i più comuni.

Attraverso l'art. 615-quinquies si mira dunque a reprimere la diffusione di questi codici maligni (indipendentemente dallo scopo per cui sono creati), e costituisce reato la distribuzione di supporti contenenti malware, o la loro diffusione attraverso reti telematiche (non è pertanto punita la creazione o la semplice detenzione di tali software).

Da precisare però che tale reato è punito solo qualora vi sia dolo e non lo è nel momento in cui si accerti una condotta meramente colposa. Ciò serve a scagionare tutti quegli individui che si vedono vittime ignare ed inconsapevoli della diffusione dei malware (con particolare riferimento agli worm, che si riproducono senza il consenso dell'utente ed a sua insaputa).

Inoltre l'art. 615-quinquies individua un reato di pericolo, in cui non necessariamente si deve verificare una distruzione (parziale o totale), come invece avviene nel caso dell'art. 635-bis (reato di evento).

Dal punto di vista della prevenzione è possibile ricorrere all'utilizzo di software quali antivirus, antispyware, ecc. che, se opportunamente aggiornati, sono in grado di segnalare all'utente l'eventuale presenza di software maligni.

Ultima macro-categoria dei reati informatici è quella inerente la riservatezza dei dati e delle comunicazioni informatiche.

In tale ambito il Codice Penale interviene con l'intento di reprimere forme di intrusione nella sfera privata altrui, in materia di riservatezza dei dati e delle comunicazioni informatiche è quello adottato con l'art. 615-ter del Codice Penale "accesso abusivo ad un sistema informatico o telematico", Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio"; art. 615-ter ("Accesso abusivo ad un sistema informatico o telematico"): "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito..".

Con questo articolo si vuole tutelare il sistema informatico, inteso qui come vera e propria estensione del domicilio dell'individuo, al fine di proteggerlo da accessi non autorizzati e da permanenza non gradita (tutela peraltro garantita dall'art. 14 della Costituzione Italiana).

Ciò che immediatamente si coglie dall'art. 615-ter è che un sistema per poter subire un accesso abusivo, deve essere protetto da una qualsivoglia forma di sicurezza (sia essa una forma di protezione logica – ad esempio nome utente e password - o fisica – vigilantes o porte blindate a protezione dei sistemi informatici; ed è d'altronde questo il caso in cui si può applicare il punto due del secondo comma), e ciò presuppone un palesato interesse dell'individuo a voler tutelare i propri dati (ed in ciò si distingue anche la differenza del domicilio informatico da quello "reale" tutelato dall'art. 614 c.p.; essendo infatti il domicilio informatico un "luogo" estremamente flessibile ed aperto, non si può tutelare il domicilio a priori in quanto tale, ma si deve tutelare solo ciò che esplicitamente il titolare ha deciso che deve rimanere riservato, e tale volontà esplicita è manifestata attraverso l'adozione di una misura di sicurezza).

Nel caso infatti in cui il sistema informatico non sia protetto in alcun modo non può sussistere il reato di accesso abusivo.

Da precisare inoltre che con l'art. 615-ter non si fa alcun riferimento ad eventuali danni causati dall'accesso abusivo al sistema (questione già affrontata con l'art. 635-bis), ma si mira a reprimere esclusivamente l'atto di accesso ad un sistema per il quale non si hanno i diritti per accedervi o per permanervi oltre la durata stabilita dal titolare del sistema.

Ciò che dunque appare importante alla luce dell'art. 615-ter è la salvaguardia dei dati contenuti all'interno del proprio "domicilio" informatico.

Dal punto di vista della prevenzione appare evidente che tra le possibili soluzioni per scongiurare un accesso abusivo, ci sia quella di regolare l'accesso per selezione (o, di contro, per esclusione).

A tal riguardo una delle più semplici misure da adottare è quella di impostare un account dotato di nome utente e password di accesso. Altra soluzione, più dispendiosa ma anche più efficace, è quella di dotarsi di un firewall al fine di controllare gli accessi.

In ogni caso, come già specificato, occorre che sia presente un, seppur minimo, sistema di protezione al fine di poter parlare di accesso abusivo in relazione all'art. 615-ter c.p.

Altre disposizioni del Codice Penale in materia di riservatezza dei dati e delle comunicazioni informatiche, le si possono riscontrare nell'art. 615-quater:("Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici"): "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con ……..

Anche l'art. 615-quater è compreso (come il 615-ter) nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio". A differenza dell'art. 615-ter però, l'art. 615-quater fa riferimento al possesso indebito ed all'eventuale diffusione di codici di accesso e non il loro utilizzo ai fini di un accesso abusivo.

Tale articolo punisce dunque la detenzione non autorizzata di codici di accesso (con codici di accesso si intendono non solo password ma anche P.I.N., smart card criptate o eventuali sistemi biometrici, come le impronte digitali ed il riconoscimento vocale), ma anche la loro diffusione illecita a terzi non autorizzati. Inoltre è contemplato quale reato anche la diffusione di istruzioni tecniche su come eludere od ottenere i suddetti codici di accesso.

In ogni caso non è sufficiente la detenzione o la diffusione di codici illeciti per poter incorrere nelle pene previste dall'articolo in questione, ma è necessario che da tale detenzione o diffusione ne derivi un profitto per sé o per altri o altresì un danno a terzi.

Sempre in riferimento alla macro-categoria sulla riservatezza dei dati e delle comunicazioni informatiche, il Codice Penale individua nell'art. 621 (Titolo XII "dei delitti contro la persona", Sezione V "dei delitti contro la inviolabilità dei segreti") un ulteriore forma di protezione della riservatezza dei propri documenti; art. 621 ("Rivelazione del contenuto di documenti segreti"):

"Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con…

Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.

Più nello specifico dell'ambito informatico entrano gli artt. 617-quater, 617-quinquies e 617-sexies (Titolo XII "dei delitti contro la persona", Sezione V "dei delitti contro la inviolabilità dei segreti"), i quali tutelano la riservatezza delle comunicazioni informatiche proprio come nello stesso Codice Penale sono tutelate le comunicazioni per mezzo di apparecchiature telefoniche, telegrafiche ed epistolari attraverso gli artt. 617 e ss. Il fine ultimo di tali articoli è comunque quello espresso attraverso l'art. 616 c.p. sulla "Violazione, sottrazione e soppressione della corrispondenza", sostenuto, tra l'altro, anche dall'art. 15 della Costituzione Italiana sulla libertà e segretezza della corrispondenza e della comunicazione.

Nello specifico gli artt. 617-quater, 617-quinquies e 617-sexies: art.617-quater ("Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche"): "Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con ...

art. 617-quinquies (“Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche”): “Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con ...

art. 617-sexies (“Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche”): “Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con...

Gli articoli si riferiscono chiaramente a tutte quelle forme di comunicazione informatica per cui è prevista una identificazione ben precisa dei/del destinatario (es. e-mail, chat dirette ad un utente preciso, ecc), in cui cioè esiste una reale forma di corrispondenza inviolabile, la quale non esiste invece per le forme di comunicazione in cui i destinatari non sono ben definibili e specificati (es. siti pubblici del world wide web, chat pubbliche, ecc.).

A tal proposito viene invece a tutela l’art. 21 della Costituzione Italiana (inerente la libertà di manifestare il proprio pensiero).

Detto ciò appare evidente come il reato di cui all’art. 617-quinquies si disponga in una posizione prodromica rispetto all’art. 617-quater, in quanto il primo si colloca in una fase antecedente l’intercettazione vera e propria e non è necessaria la prova dell’avvenuta intercettazione, interruzione o impedimento della comunicazione, essendo sufficiente accertare l’obiettiva potenzialità lesiva dell’apparecchiatura. Nel caso in cui avvenga poi l’effettiva intercettazione, interruzione o impedimento, si procederà secondo quanto previsto dall’art. 617-quater.

Con l’art. 617-sexies si mira invece a sanzionare l’impiego e la rivelazione pubblica dei contenuti precedentemente intercettati, nonché la loro falsificazione, alterazione o soppressione a scopo di profitto o a danno di altri, condizione necessaria perché sussista il reato.

Da precisare poi, ai fini soprattutto dell’art. 617-quater, che l’intercettazione si verifica nel momento in cui si carpisce, in maniera fraudolenta ed all’insaputa dei soggetti coinvolti nella comunicazione, il contenuto del messaggio trasmesso. Qualora i soggetti coinvolti nella comunicazione autorizzino l’intercettazione il reato non sussisterebbe.

In ogni caso, perché si possa parlare di “intercettazione”, il messaggio deve giungere integralmente al suo destinatario previsto; in caso in cui il messaggio non giunga al destinatario ma venga interrotto lungo il suo cammino si parlerebbe di “interruzione”; nel caso in cui invece la comunicazione non potesse nemmeno partire si parlerebbe di “impedimento”.

Tra le principali tipologie di reati che possono rientrare negli articoli di cui sopra, e specificatamente nell’art. 617-quater, vi è lo Sniffing, una tecnica finalizzata a carpire i dati e le informazioni che attraversano una rete telematica.

Dal punto di vista preventivo la miglior soluzione per proteggersi da eventuali intercettazioni di comunicazioni informatiche, operate attraverso attacchi sniffing od altre modalità, è quella di adottare tecniche crittografiche che consentano di rendere illeggibile il contenuto del documento a chi è privo dell’autorità per farlo.

art. 623-bis (“Altre comunicazioni e conversazioni”): “Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati.”

Con l’art. 623-bis si vuole semplicemente estendere il campo di riferimento degli articoli sin qui discussi (ed appartenenti alla sezione “dei delitti contro la inviolabilità del domicilio”) a qualunque tipo di trasmissione, sia essa, indifferentemente, di dati, suoni o immagini.

Analisi dei rischi

Un’accurata analisi dei rischi ai quali è esposto l’ente richiede uno specifico intervento; viene evidenziata una sintesi delle minacce più comuni e delle funzioni di sicurezza ritenute necessarie, con particolare riguardo agli aspetti tecnologici.

I rischi possono essere raggruppati in termini di:

- rischi per la riservatezza: le informazioni e i documenti devono essere accessibili ed utilizzate solo da, persone e/o da responsabili esterni, debitamente autorizzati e per fini conformi agli obiettivi e finalità dell’ente;
- rischi per la integrità: i dati e i documenti devono essere esatti, aggiornati, corrispondenti alla realtà e protetti da qualsiasi forma di alterazione non controllata;
- rischi per la disponibilità: l’accesso ai dati e ai documenti deve poter avvenire ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;
- rischi di uso improprio: l’accesso ai dati deve avvenire esclusivamente per i fini definiti dal Titolare da parte di soggetti adeguatamente autorizzati ed istruiti.

Sulla base della suddetta classificazione nella tabella seguente vengono identificati, per ciascuna risorsa critica, i rischi per i quali devono essere adottate misure di sicurezza adeguate.

Rischio Risorsa	Riservatezza	Integrità	Disponibilità	Uso improprio
Sistema informatico (server, PC)	Diffusi Trafugati Inferenza	Errore utente Errore Hw Errore Sw Manomissione Virus informatici	Cancellati Mal inseriti Distrutti	Fini incongruenti Uso improprio Non accessibili Non bloccabile
Documenti cartacei	Diffusi Trafugati Inferenza	Modifica Manomissione	Persi Distrutti	Fini incongruenti Uso improprio Non accessibili
Locali e strutture logistiche	Guasto Distruzione Manomissione	Guasto Distruzione Manomissione	Guasto Distruzione Manomissione	

Trattamenti esterni	Diffusi Trafugati Inferenza	Errore utente Errore Hw Errore Sw Manomissione	Non disponibile	Fini incongruenti Non bloccabile

Misure di sicurezza

A fronte dell'analisi dei rischi, sono individuati specifici interventi operativi per la sicurezza così articolati:

- misure di sicurezza fisiche riguardanti la sicurezza passiva ed il controllo accessi ai locali dell'ente finalizzate alla salvaguardia degli strumenti informatici, i supporti di memorizzazione dei documenti informatici e di conservazione dei documenti cartacei
- misure di sicurezza logiche riguardanti il controllo dell'accesso al sistema informatico
- misure organizzative relative ai ruoli e alle responsabilità dei vari soggetti, interni ed esterni, che gestiscono documenti e trattano dati personali

Misure Fisiche

Controllo accessi

L'accesso alle postazioni pc, agli uffici e agli archivi è riservato al personale autorizzato. L'accesso del personale esterno deve essere motivato da esigenze tecniche od organizzative ed è consentito sotto la responsabilità del personale interno abilitato ed autorizzato dal Titolare.

Le apparecchiature informatiche o gli archivi cartacei non sono, di norma, collocati in aree aperte o comunque accessibili al pubblico. I server di rete sono collocati in locali accessibili tramite una porta con serratura a chiave. Le chiavi sono in possesso del personale abilitato e del Titolare.

Gli archivi operativi devono normalmente essere mantenuti chiusi. Gli archivi del personale (fascicoli cartacei personali) sono custoditi in apposito ufficio chiuso a chiave il cui accesso è consentito solo agli incaricati.

Sistema antincendio e di messa a terra

Tutto l'edificio è dotato di mezzi antincendio mobili azionabili manualmente dal personale operante, appositamente incaricato, addetto alla gestione dell'emergenza (ai sensi del D. Lgs. n. 81/2008), di impianto per la rilevazione incendi e delle compartimentazioni necessarie al controllo di eventi dannosi, nonché della verifica dell'impianto di messa a terra e dell'impianto elettrico in generale.

Misure Logiche

Le misure di sicurezza logiche riguardano i criteri che devono essere seguiti dai diversi programmi software, di sistema o applicativi, per controllare (vale a dire selezionare e/o limitare) l'accesso degli utilizzatori alla rete locale, alle interconnessioni esterne internet, ai server dati ed applicativi e alle funzionalità applicative.

Controllo accesso ai sistemi di elaborazione

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento. Inoltre per i dipendenti pubblici, così come previsto dalla normativa di settore, è vietato un utilizzo a fini privati di materiali o attrezzature di cui dispone per ragioni di ufficio

L'accesso diretto, o in accesso remoto, agli elaboratori e ai server di rete locale è consentito esclusivamente al titolare o ai suoi incaricati, previa autorizzazione del Titolare.

L'accesso alle risorse informatiche, locali o di rete, avviene attraverso uno specifico profilo di abilitazione. Tale profilo definisce, per ogni soggetto associato (qualsiasi utente del sistema informatico, interno o esterno), le funzionalità disponibili ed in particolare le seguenti tipologie di abilitazioni di accesso:

- accesso locale alle stazioni di lavoro
- accesso alla rete locale tramite la stazione di lavoro
- accesso ai trattamenti e/o gli archivi presenti sui server della rete locale per cui viene data abilitazione con specifici diritti (sola lettura, modifica, ecc.)
- la possibilità di interconnessione con reti esterne, in particolare Internet e posta elettronica.

La presenza di archivi e documenti sulle singole postazioni di lavoro deve essere considerata eccezionale, a fronte di esigenze particolari per elaborazioni individuali, che vanno preventivamente concordate con il titolare.

Qualsiasi tipo di dato/documento attinente i trattamenti svolti dal soggetto va mantenuto presso aree ad accesso controllato situate, di norma, sui file server dell'ente o sul file server dell'applicativo di gestione. Non è consentito dalle singole stazioni di lavoro condividere archivi senza il consenso del titolare.

Gli aspetti di sicurezza circa l'accessibilità ed integrità degli archivi locali sono a carico dell'incaricato che opera nella stazione di lavoro, il quale, per il suo corretto utilizzo, dovrà attenersi alle specifiche direttive predisposte dal Titolare del trattamento.

Il sistema di controllo accessi delle stazioni di lavoro garantisce:

- l'accesso agli archivi eventualmente presenti sulle stazioni di lavoro esclusivamente ai soggetti identificati dal titolare;

- l'accesso alla rete è riservato esclusivamente ai soggetti autorizzati ed attraverso la o le stazioni di lavoro cui lo stesso è abilitato;
- l'accesso agli archivi ed alle applicazioni presenti sul server locale esclusivamente ai soggetti abilitati e per le funzionalità autorizzate;
- l'accesso in remoto deve essere autorizzato dal Titolare del trattamento il quale stabilirà con atto scritto i tempi, le modalità e le limitazioni a cui sono sottoposti tali accessi nonché le misure di sicurezza richieste, il titolare potrà in ogni momento chiedere di interrompere gli accessi;

Identificazione ed Autenticazione degli utenti

Ogni utilizzatore del sistema informatico dell'ente è identificato mediante un codice personale user-id (dato pubblico) e una password (dato privato), assegnati e gestibili dal Titolare e/o dall'Amministratore di sistema ove nominato, che permettono l'accesso alle stazioni di lavoro ed alla rete locale secondo i diversi profili di abilitazione.

La User-id ha una composizione standardizzata per tutti gli utenti del sistema. Lo stesso codice non può, neppure in tempi diversi, essere assegnato a persone diverse. Ad ogni codice è possibile associare uno o più profili di abilitazione.

In caso di revoca dell'incarico e/o modifica delle autorizzazioni, il codice identificativo dell'autorizzato è immediatamente reso inutilizzabile o, secondo le necessità, ne viene modificato il profilo delle abilitazioni associate.

Password

Ad ogni user-id è associata una password. Al primo utilizzo, l'incaricato del trattamento ha l'obbligo di modificarla tenendo presenti le direttive dell'Amministratore di sistema e le seguenti regole:

- deve essere alfanumerica, di non meno di 8 caratteri di cui almeno 1 numerico, uno maiuscolo e un simbolo
- non deve essere composta utilizzando la user-id
- non deve essere ottenuta anagrammando la precedente password
- non deve essere ottenuta utilizzando il proprio nome e data di nascita
- deve essere sostituita almeno ogni tre mesi in caso di trattamento di particolari categorie di dati
- La password in uso dovrà essere trascritta, sigillata in busta chiusa e consegnata al custode delle password se nominato o al titolare, la password consegnata verrà utilizzata solo per motivi di estrema urgenza o controllo da soggetti preposti. (titolare e autorità competenti)

Ogni autorizzato in base al proprio profilo di abilitazione, accede alle postazioni di lavoro di riferimento e alle applicazioni di rete, sia internet sia intranet (applicativi gestionali), per determinati applicativi è prevista una seconda autenticazione.

Screen saver

Le postazioni di lavoro utilizzate sono dotate di funzione salva schermo (screensaver) protetto da password che si attiva dopo 3 minuti (valore massimo tollerato) di inattività. E' quindi inibito un utilizzo improprio di dati personali in caso di abbandono, anche temporaneo, della stazione già abilitata all'accesso.

E' fatto divieto di trascrivere su carta o memorizzare su supporto magnetico, salvo utilizzando procedure concordate con il titolare, la password di accesso ai sistemi informatici. E' fatto divieto, altresì, di comunicare la password ad altri, anche per solo utilizzo temporaneo od in caso di emergenza.

Al momento dell'attivazione di un nuovo codice identificativo il titolare assegna una password provvisoria che comunica solo all'utilizzatore interessato; quest'ultimo avrà l'obbligo, al primo accesso, di cambiare la password provvisoria con un'altra idonea secondo le regole sopra esposte.

Controllo accessi alla rete, ai sistemi di elaborazione, ai programmi applicativi, ai dati

Gli accessi alle risorse informatiche in rete sono protetti contro le intrusioni da uno specifico sistema di controllo. Ogni utente è abilitato in modo puntuale all'accesso alla rete e alle singole risorse di elaborazione necessarie per i trattamenti cui è autorizzato dal proprio "profilo utente". Di norma, nessun utente ha l'abilitazione di amministratore locale della postazione di lavoro informatica.

Protezione antivirus

Tutti gli elaboratori sono protetti contro il rischio di intrusione ad opera di programmi illeciti.

La protezione di tutte le postazioni in rete avviene in tempo reale mediante l'utilizzo di adeguati programmi antivirus, antispam ed eventuale firewall, aggiornati centralmente, in grado di monitorare il rischio di infezione. L'aggiornamento della protezione delle stazioni di lavoro avviene tramite connessione programmata all'accensione della stazione di lavoro e più volte al giorno al server antivirus interno alla rete.

Procedura in caso di anomalia rilevata o sospetta

In caso di anomalie, anche solo sospette, e/o pericoli di intrusione o modificazione nelle postazioni e impostazioni delle stesse, il lavoratore deve:

- Scollegare il cavo di rete e lasciare il pc accesso
- Avvertire prontamente il Titolare.

Backup e ripristino della disponibilità dei dati

I dati/documenti contenuti negli archivi informatici utilizzati dall'ente nella propria rete locale sono protetti contro il rischio di perdita, anche accidentale, attraverso apposite procedure di salvataggio di copie di sicurezza che garantiscano il ripristino delle informazioni entro un limite stabilito dal Titolare.
Le procedure consentono il ripristino selettivo dei dati. Periodicità dei salvataggi, numero di versioni conservate e procedure di ripristino sono state definite in modo da soddisfare le esigenze di sicurezza dell'ente.

Criteri e procedure di rilascio di user-id e password

Al lavoratore o gruppo di lavoro vengono attribuiti dal titolare in base al profilo utente individuato nella comunicazione di incarico, un codice identificativo (user-id) ed una password iniziale per l'accesso e l'utilizzo degli archivi e servizi applicativi.

Criteri e procedure di controllo accessi agli archivi informatici

L'accesso al sistema e alle risorse di rete può essere controllato da un apposito sistema di gestione che, sulla base delle abilitazioni corrispondenti ai vari profili utente, consente l'accesso ai soli archivi/dati necessari e sufficienti per il trattamento. In ogni caso il Titolare, eventualmente tramite suoi incaricati, ha il compito di vigilare sul corretto utilizzo delle procedure.

Criteri e procedure di controllo accessi agli archivi cartacei

L'accesso agli archivi cartacei contenenti dati sensibili e/o particolari è controllato e selezionato sulla base delle necessità di trattamento. Gli Autorizzati interni od esterni all'organizzazione che accedono a tali archivi devono conservare i documenti prelevati e restituirli al termine deltrattamento.

E' fatto divieto di produrre copie anche parziali dei documenti contenenti dati sensibili e/particolari, salvo diverse esplicite disposizioni relative a procedure per cui le copie sono indispensabili. Tutte le copie vengono trattate con le stesse misure di riservatezza e sicurezza degli originali e distrutte dopo l'uso dallo stesso incaricato al trattamento dei dati contenuti.
L'accesso agli archivi di riposo segue le norme previste per le aree di sicurezza ed è consentito esclusivamente agli incaricati specificatamente autorizzati. Il prelievo dei documenti deve essere registrato riportando i dati relativi al soggetto richiedente, data di uscita, data di restituzione.

Criteri e procedure per l'utilizzo della posta elettronica e di Internet

I servizi di posta elettronica e di navigazione internet sono risorse dell'ente, che il datore di lavoro mette a disposizione del dipendente per il perseguimento dei fini lavorativi. Pertanto l'utilizzo di tali strumenti è consentito per svolgere gli incarichi per i quali sono state assegnate le abilitazioni di accesso, con riferimento alle attività del personale. L'uso improprio di tali strumenti può pregiudicare in modo rilevante la sicurezza dei dati/documenti trattati, arrecando rilevanti danni, anche sotto il profilo penale, all'attività dell'ente.

Per garantire gli adempimenti di sicurezza previsti dalla normativa vigente, il gestore tecnico del servizio (service provider) registra le informazioni relative all'utilizzo degli strumenti di posta elettronica e Internet. Tali informazioni sono a disposizione esclusivamente delle autorità giudiziarie preposte e memorizzate in forma protetta per il tempo stabilito dalle normative di riferimento.

In ogni caso sono impartite ai dipendenti le seguenti istruzioni:

- gli utenti non devono salvare password fisse nei loro browser o e-mail a meno che il PC preveda password di accessione o log on e lo screen saver sia protetto con password

- tutte le attività in Internet devono passare da punti di accesso approvati
- tutte le modifiche al software e hardware di componenti del sistema di sicurezza informatica devono essere approvate preventivamente, e quindi installate, da un tecnico abilitato ed eventualmente dall'Amministratore di sistema se nominato
- non si possono attivare connessioni di rete verso l'esterno, via Internet o altri sistemi, che non siano stati preventivamente autorizzati dal Titolare
- è fatto divieto di utilizzare le caselle di posta elettronica ordinaria nominative o di gruppo per comunicazioni non strettamente correlate all'attività lavorativa.
- non è consentito comunicare le proprie credenziali (userid, email) a siti e servizi internet, se non preventivamente autorizzati dal Titolare

Criteri e procedure per i supporti rimovibili e apparecchiature portatili

Relativamente ai supporti rimovibili e alle apparecchiature portatili sono impartite agli incaricati di trattamento le seguenti istruzione:

- non utilizzare supporti rimovibili o apparecchiature portatili personali (e di sistemi elettronici e telematici personali, in genere). I soli supporti rimovibili e i sistemi elettronici e telematici ammessi nell'ente sono quelli espressamente autorizzati, nel rispetto delle specifiche procedure organizzative e gestionali, dal titolare.
- tutti i supporti magnetici utilizzati possono essere inizializzati prima dell'uso mediante apposite procedure indicate dal titolare, che consentano di rendere illeggibili i dati eventualmente registrati in precedenza. Tali procedure si applicano anche in caso di eliminazione dei supporti magnetici rimovibili.
- è fatto divieto di portare all'esterno dell'ente qualsiasi supporto rimovibile fornito se non espressamente autorizzati.
- le apparecchiature portatili saranno consegnate previa esplicita richiesta per esigenze di servizio. Tutte le apparecchiature portatili sono soggette al regolamento cui sono soggette le normali postazioni di lavoro. Prima di collegare le apparecchiature portatili a reti diverse da quella dell'ente o a dispositivi esterni occorre essere preventivamente autorizzati.

Dispositivi mobili di proprietà (personali)

E' vietato l'utilizzo di dispositivi mobili di proprietà e l'utilizzo di sistemi di comunicazione (quali ad esempio whatsapp, ecc), ovvero questi sono consentiti, per comunicazioni personali urgenti, nel limite del rispetto della riservatezza dei dati degli interessati afferenti all'ente.

L'utilizzo dei social non è permesso in orario di lavoro e non deve coinvolgere in nessun modo i dati personali degli interessati coinvolti nelle attività dell'ente (si ricorda che: chi diffonde dati nei social network assume il ruolo di titolare del trattamento di fatto assumendo la piena responsabilità ed effettuando un trattamento illecito se non autorizzato dall'interessato, reato penale, e cede la proprietà dei dati al gestore del social)

Utilizzo dei telefoni, fax, scanner e fotocopiatrici

Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso dell'Ente a disposizione.

Qualora venisse assegnato un cellulare dall'Ente all'utente, (la concessione dell'utilizzo del cellulare viene rilasciata dalla Direzione) quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono dell'Ente: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare dell'Ente è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite digitando il prefisso per l'addebito delle chiamate personali.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

È vietato l'utilizzo di scanner per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

Misure Organizzative

"Autorizzati" al trattamento dei dati

I dipendenti che trattano dati personali sono formalmente incaricati dal datore di lavoro tramite comunicazione scritta che definisce gli archivi cui l'incaricato può accedere ed i trattamenti che è autorizzato ad effettuare, identificando il profilo utente che definisce le abilitazioni nel sistema di controllo accessi al sistema. E compito dell'incaricato verificare in ogni momento l'adeguatezza dell'utilizzo e dell'accessibilità agli archivi cartacei e informatici perciò avrà cura di non lasciare incustoditi gli archivi senza attivare le debite protezioni e di assicurarsi di spegnere tutte le macchine (pc, stampanti, ecc...) e assicurare la chiusura di armadi, porte degli archivi cartacei e dell'ente al termine del lavoro e abbandono dell'ufficio.

Nel caso che trattamenti di dati personali di cui sia titolare l'ente siano affidati a soggetti esterni nell'ambito dell'esecuzione di contratti di fornitura di beni o servizi si procede, con atto separato o attraverso l'inserimento di apposita clausola nel contratto, alla nomina del soggetto esterno a Responsabile del trattamento.

E' compito del Responsabile esterno provvedere al trattamento dei dati, nel rispetto della normativa vigente Privacy, nell'ambito della sua organizzazione.

Al Responsabile esterno viene eventualmente richiesta, congiuntamente all'accettazione dell'incarico, copia dei propri Documenti afferenti le Misure minime di Sicurezza, analisi d'impatto e altri documenti utili all'analisi e alla valutazione della compliance tra aziende.

I dipendenti o i soggetti esterni che sono addetti alla manutenzione dei sistemi elettronici (elettronica di rete, server, PC, etc.) sono autorizzati per iscritto dal Titolare del trattamento e devono attenersi alle specifiche disposizioni in materia di sicurezza loro comunicate.

Amministratore di sistema

Con specifico atto l'ente può nominare gli amministratori di sistema in conformità al provvedimento del Garante per la protezione dei dati personali 27 novembre 2008 avente ad oggetto: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Il ruolo di Amministratore di sistema è svolto dal personale tecnico cui competono le attività di amministrazione e gestione delle risorse informatiche.

Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Regolamento UE 2016/679.

Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione dell'Ente, tramite il personale dei Servizi Informatici o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Sistemi di controlli graduali

In caso di anomalie, il personale incaricato dei Servizi Informatici effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti dell'Ente e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e per i casi di particolare gravità solo su autorizzazione della Direzione. Tutti coloro che utilizzano le strumentazioni informatiche e telematiche devono sempre considerare che le apparecchiature utilizzate immagazzinano una serie di informazioni inerenti il loro uso: numero di mail inviate e ricevute; siti web visitati (url); pagine visualizzate; durata delle connessioni a Internet; materiale scaricato.

In particolare, il sistema informativo fornisce una serie di informazioni inerenti l'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro (log), quali:

I log di accesso a internet

I log inerenti la posta elettronica I log relativi ai virus rilevati

I log inerenti l'accesso alle banche dati e gli applicativi

Log degli applicativi installati sulla propria postazione di lavoro

Tutte le suddette informazioni potrebbero servire all'Ente per poter salvaguardare il proprio patrimonio informativo e tecnologico o per rispondere a richieste dall'autorità giudiziaria.

I controlli verranno posti in essere solo per gruppi aggregati.

Nel caso in cui si riscontrassero comportamenti potenzialmente dannosi e comunque non conformi alle suddette linee guida, la Direzione provvederà a informare il dirigente responsabile del servizio. Nel caso in cui si sospettassero illeciti di rilevanza penale si provvederà a denunciare il fatto all'autorità giudiziaria.

A seguito di comportamenti potenzialmente dannosi, l'Amministrazione si riserva di adottare le contromisure ritenute idonee per limitare i possibili effetti.

In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati senza autorizzazione.

Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento e alle norme comportamentali ivi contenute. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Verifiche iniziali di cyber-security

1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro dell'ente.
2. I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3. Sono individuate le informazioni, i dati e i sistemi critici per l'ente affinché siano adeguatamente protetti.
4. È stato nominato un referente, a discrezione del Titolare, che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5. Sono rispettate le leggi e/o i regolamenti con rilevanza in tema di cyber-security che risultino applicabili per l'ente.
6. Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7. Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8. Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9. Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10. Il personale è adeguatamente sensibilizzato e formato sui rischi di cyber-security e sulle pratiche da adottare per l'impiego sicuro degli strumenti dell'ente (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici hanno cura di predisporre per tutto il personale dell'ente la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11. La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto e responsabile. Le credenziali di accesso di default sono sempre sostituite.
12. Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'ente. I backup sono conservati in modo sicuro e verificati periodicamente.
13. Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14. In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15. Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

CASA DI RIPOSO CARTIGLIANO

Verifiche periodiche del sistema informatico

Data Verifica	
Modificare con cadenza almeno trimestrale la password di accesso al computer	
Verificare con cadenza almeno trimestrale che ogni utente abbia lo screen saver con password attivato	
Assistere gli incaricati del trattamento dati nelle operazioni di modifica delle password	
Verificare con cadenza almeno trimestrale che sia attivo l'aggiornamento dei programmi di protezione antivirus	
Verificare con cadenza almeno trimestrale l'avvenuto aggiornamento dei sistemi operativi	
Verificare con cadenza almeno trimestrale il sistema di protezione anti-intrusione (firewall se presente)	
Verificare con cadenza almeno semestrale la qualità dei backup e l'affidabilità dei supporti rimovibili, tramite delle prove di ripristino dati	
Verificare con cadenza almeno semestrale la funzionalità del gruppo di continuità	
Verificare con cadenza almeno annuale la cifratura del computer e dei supporti di backup	
Provvedere quando necessario all'aggiornamento del sistema di autenticazione e di autorizzazione degli incaricati e farne comunque una verifica almeno una volta all'anno	
Controllare la scadenza del contratto di assistenza tecnica per il ripristino del computer in caso di guasto	
Effettuare almeno una volta all'anno la pulizia fisica interna del computer	
Verificare almeno una volta all'anno la qualità dei supporti di backup e sostituirli se necessario	

La Comunicazione WEB

L'ente pone grande attenzione alla comunicazione web attraverso il sito o altre forme di comunicazione telematica che offrono grandi possibilità di comunicazione in tempo reale e servizio agli utenti ma che possono anche porre a rischio il trattamento dei dati. La costruzione del sito e la sua manutenzione è affidata a professionista specializzato che ne cura il continuo aggiornamento.

Il consenso

Il consenso, se necessario, che deve essere espresso nelle forme previste dalla legge, viene precisato a tutti i soggetti coinvolti nell'organizzazione che il consenso deve comprendere le caratteristiche di:

1) inequivocabile;
2) libero;
3) specifico;
4) informato;
5) verificabile;
6) revocabile.

1) Consenso inequivocabile (unambiguous nella versione inglese) vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate). Cioè deve prevedere una chiara azione positiva (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).

Il Considerando 32 del GDPR recita: "il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Il consenso deve, invece, essere esplicito (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione).

Occorre dire che la versione originaria della proposta della Commissione europea prevedeva sempre il consenso esplicito, poi si è pervenuti al compromesso attuale.
Il consenso esplicito si può avere con una dichiarazione scritta e firmata dall'interessato o tramite l'invio di un'email indicante che la persona accetta espressamente il trattamento di determinate categorie di dati, oppure raccogliendo il consenso in due passaggi: inviare un'email all'interessato, che poi dovrò confermare la prima azione di consenso.

2) Il consenso deve essere dato liberamente, significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso. L'articolo 7 del GDPR chiarisce che "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".
Ad esempio, nel caso di pubblicità commerciale, il consenso deve essere separato rispetto al consenso per la prestazione contrattuale richiesta, l'utente deve avere la possibilità di addivenire al contratto senza dover subire il ricatto di dover ricevere pubblicità commerciale. Non può definirsi libero il consenso a ulteriori trattamenti dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta (provvedimento del Garante del 31 gennaio 2008).

Questo purtroppo porta al rischio che molti dei consensi ottenuti dai servizi online possano essere ritenuti invalidi. Lo stesso Gruppo Articolo 29 fornisce un esempio chiarificatore: una app mobile per il foto-ritocco chiede il consenso per accedere alla geo-localizzazione e i dati vengono utilizzati a fini di pubblicità comportamentale. Ma né la geo-localizzazione, né la pubblicità sono necessari per la fornitura del servizio (foto-ritocco), per cui subordinare l'uso della App a tale consenso rende il consenso non libero e quindi illecito.

Sul punto la Corte di Cassazione italiana, con la sentenza n. 17278/2018, ha precisato che il gestore di un sito concernente un servizio fungibile e rinunciabile può negare l'accesso al servizio all'utente che non acconsenta ai trattamenti dei propri dati per finalità commerciali. In questo caso il punto focale sta nella fungibilità e nel poter rinunciare liberamente al servizio. Il blocco dell'accesso al sito non potrebbe essere imposto nel caso in cui il sito offra un servizio essenziale per l'utente. La Corte sostiene che ciò che è interdetto al gestore di "utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia la volontà di riceverli".
Il Garante ha, però, ribadito, successivamente, col provvedimento del 12 giugno 2019, che la libertà del consenso "non è assicurata né quando viene richiesto un unico consenso per più diverse finalità di trattamento, né quando si assoggetta la fruizione di un servizio […] alla previa autorizzazione a trattare i dati conferiti, ai fini di tale servizio, per finalità diverse qual è quella di promozione e quella statistica". In tal senso appare un evidente contrasto tra Suprema Corte e Garante.

Un altro problema riguarda il consenso dei dipendenti. Se il datore di lavoro richiede il consenso all'utilizzo del dato (es. vuole pubblicare la foto dei dipendenti sul sito web ente) e vi è un pregiudizio reale o potenziale per il cliente non consenziente (cosa altamente probabile in un contesto lavorativo), il consenso non può ritenersi valido

perché non libero. Dato lo squilibrio di potere tra datore e dipendente, quest'ultimo può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

3) Il consenso deve essere specifico, cioè relativo alla finalità per la quale è eseguito quel trattamento (granularità del consenso). Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso. Per cui avremo un consenso per il marketing diretto, un consenso per la profilazione, ecc…
Nel caso di titolari congiunti ogni titolare deve acquisire il consenso relativamente alle proprie finalità. Ad esempio, il gestore di un sito web che utilizza plug-in di Facebook dovrà chiedere il consenso con riferimento alla sola raccolta dei dati e successiva comunicazione a Facebook.

Un caso classico riguarda i cookie. Il consenso deve essere specifico in relazione alla finalità dei cookie, non può essere unico per tutti i cookie se questi hanno finalità differenti.

4) Il consenso deve essere informato, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso (ad esempio deve essere indicato che in assenza di consenso non potrà accedere a determinate sezioni del sito web). L'informazione si ha attraverso l'apposita informativa, che in questo caso diventa una vera e propria condizione di legittimità del trattamento. Il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

5) Consenso verificabile non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta (anche se in alcune ipotesi -es. dati sensibili- può essere preferibile perché consente più facilmente di provare il consenso, facilitando quindi le verifiche da parte dell'autorità), ma che l'ente deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti). L'ente dovrà essere in grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.
Il WP29 suggerisce di utilizzare un registro nel quale siano conservate le informazioni relative alla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso, e una copia delle informazioni presentate all'interessato in quel momento.

6) Il consenso deve essere revocabile in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento.

Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito form sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa (interpello al titolare). Nel caso in cui il titolare non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

Con la revoca si innesca il diritto di cancellazione, per cui l'ente deve cancellare i dati dell'utente. Ovviamente vi sono motivi legittimi in base ai quali un ente ha necessità di conservare alcuni dati dell'utente anche dopo la revoca del consenso, come ad esempio mantenere un registro delle transazioni per motivi fiscali o altri dati. In ogni caso l'ente può avvertire l'interessato che a seguito della revoca del consenso, vi sarà la cancellazione dei dati è la conseguente impossibilità di fornire ulteriori servizi.