

**Art. 24-bis**

*Delitti informatici e trattamento illecito di dati*

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

## ARTICOLI CITATI

Art. CODICE PENALE	Testo
<b>491-bis</b> Art. 491-bis c.p. Documenti informatici.	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.
<b>615-ter</b> Accesso abusivo ad un sistema informatico o telematico.	<p>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 la reclusione fino a tre anni.</p> <p>La pena è della reclusione da uno a cinque anni:</p> <p>1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;</p> <p>2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;</p> <p>3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.</p> <p>Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.</p> <p>Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.</p>
<b>615-quater</b> 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 la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.
<b>615-quinquies</b> Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.	Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

<p><b>617-quater</b> Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.</p>	<p>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 la reclusione da sei mesi a quattro anni.</p> <p>Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.</p> <p>I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.</p> <p>Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:</p> <ol style="list-style-type: none"> <li>1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;</li> <li>2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;</li> <li>3) da chi esercita anche abusivamente la professione di investigatore privato.</li> </ol>
<p><b>Art. CODICE PENALE</b></p>	<p><b>Testo</b></p>
<p><b>617-quinquies</b> c.p. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.</p>	<p>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 la reclusione da uno a quattro anni.</p> <p>La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.</p>
<p><b>635-bis</b> Danneggiamento di informazioni, dati e programmi informatici.</p>	<p>Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.</p> <p>Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.</p>
<p><b>635-ter</b> Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.</p>	<p>Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.</p> <p>Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.</p>

	Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
<b>635-quater</b> Danneggiamento di sistemi informatici o telematici.	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata
<b>635-quinquies</b> Danneggiamento di sistemi informatici o telematici di pubblica utilità.	Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
<b>640-quinquies</b> Frode informatica del soggetto che presta servizi di certificazione di firma elettronica.	Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

ASTEM SPA opera innanzitutto su propri sistemi informativi ai fini dei propri svolgimenti gestionali, ed interagisce con sistemi informatici di terzi (INPS, Agenzia Entrate, ANAC, Poste, Banche ...).

Si potrebbe verificare il caso in cui, al fine di rappresentare a terzi una situazione di ASTEM SPA differente da quella reale (ad indebito vantaggio di ASTEM SPA stessa), si intervenga come sopra rappresentato alterando dati, manomettendo sistemi, interrompendo comunicazioni ecc.

Si rinvia anche al reato di frode informatica ex art 24 DLgs 231 / 2001.

---

ASTEM SPA gestisce una mole molto rilevante di informazioni attraverso gli archivi cartacei ed il proprio sistema informatico. In quanto azienda pubblica, ASTEM SPA è tenuta a garantire al cittadino la trasparenza delle proprie operazioni e, quindi, la massima rintracciabilità dei documenti e delle informazioni ma anche il rispetto della loro privacy e, per ovvi motivi di mercato, la riservatezza dei propri dati di *business*.

Il processo di gestione dei documenti e dei dati coinvolge trasversalmente tutti gli altri processi di ASTEM SPA.

- a) La gestione del sistema informatico in generale, per quanto riguarda il rispetto della tutela dei dati personali, il corretto utilizzo degli strumenti informatici ed il rispetto della riservatezza aziendale, trova la sua descrizione nella procedura e nei protocolli di gestione dei documenti e dei dati, in particolare

nelle schede di trattamento dei dati (che identificano responsabilità e limiti di autorizzazione al trattamento) e nel Registro dei trattamenti (ex Regolamento UE 2016 / 679).

- b) Il Responsabile aziendale competente trasmette all'OdV, al momento del completamento ed annualmente, il Registro dei Trattamenti, l'Elenco aggiornato degli incaricati (interni ed esterni) e degli Amministratori di Sistema (contenente la definizione degli ambiti di responsabilità di ognuno), i quali sono oggetto di perfezionamento e di affinamento continuo.

La gestione dei sistemi informativi di ASTEM SpA è ad oggi affidata alla società A2A smart city; le relative prestazioni sono individuate in specifico contratto, agli atti di ASTEM SpA (la società deve essere individuata quale responsabile esterno del trattamento).

La gestione dei livelli di accesso ai sistemi informativi, la politica in materia di password, la gestione dei back up dei sistemi informativi ecc devono essere svolti coerentemente con gli standard previsti nel documento di cui sopra.

Ai fini del presidio alla commissione dei reati in questione, si evidenzia che la gestione dei dati e dei documenti aziendali si fonda sul sistema di protocollo aziendale attivo in ASTEM SPA.

Ai documenti protocollati e salvati in formato digitale è abbinato un archivio cartaceo aziendale per i documenti protocollati sia in entrata sia in uscita-

Il Sistema informatico (software) viene mantenuto in efficienza e sicurezza anche grazie all'intervento di soggetti esterni specializzati, tutti nominati quali Amministratori di Sistema.

I destinatari del presente Modello organizzativo devono costantemente applicare le disposizioni aziendali formulate per garantire il rispetto delle norme sulla privacy e sul corretto utilizzo degli strumenti informatici; in particolare, chiunque gestisca documenti e dati nell'ambito lavorativo, deve conoscere ed applicare i contenuti di quanto sopra sub a) e b), oltre che in generale degli altri strumenti della privacy policy e dell'informatica aziendale e del Codice etico e comportamentale.

Per esigenze di tutela del patrimonio, di sicurezza sul lavoro, di prevenzione incendi ed infortuni è stato installato un sistema audiovisivo a circuito chiuso, consistente in telecamere dislocate in aree della sede. Le videocamere sono collegate a sicuri impianti di registrazione dove le immagini ed i suoni verranno conservati per una durata massima compatibile con la normativa ed i provvedimenti vigenti del Garante della Privacy.

Tutti i dipendenti e membri di organi sociali, nonché i consulenti ed i partner, rispettano principi tali da evitare la possibilità, in generale, che siano commessi i reati di falso e, in particolare, che ciò avvenga attraverso una modalità informatica. È quindi assolutamente vietata la trasmissione di qualsiasi atto non veritiero, contraffatto o non autentico attraverso un invio telematico.

Infine, in linea generale, qualora si evidenziasse una qualsiasi criticità, il personale e i consulenti coinvolti dovranno immediatamente informare l'Organismo di Vigilanza.

---

Possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici in ogni ambito aziendale, per ciascun servizio / attività affidata nonché nell'ambito della struttura amministrativa, in quanto è ormai diffuso l'utilizzo delle tecnologie e dei sistemi informativi.

ASTEM SPA ha predisposto appositi presidi organizzativi e si è dotata come sopra descritto di adeguate soluzioni di sicurezza, in conformità alle disposizioni in materia di tutela di dati personali (Regolamento UE 2016 / 679, DLgs 101 / 2018, DLgs 196 / 2003), per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali e dei terzi.

I presidi di cui al presente capitolo si applicano a tutte le funzioni coinvolte nella progettazione, realizzazione, gestione dei sistemi informatici e del patrimonio informativo, o che vi accedono anche in rapporto con utenti

e terzi che a loro volta accedono ai sistemi di ASTEM SPA, o che svolgono interventi volti a tutelare detti sistemi ed informazioni.

Dette unità organizzative aziendali sono tenute ad osservare le disposizioni di legge esistenti in materia, la normativa interna nonché le previsioni del Codice etico e di comportamento vigente.

Più in particolare:

- ASTEM SPA predispone e mantiene aggiornato il censimento degli applicativi e/o dei *software* in uso in ogni unità organizzativa aziendale;
- l'installazione di applicativi e software e / o l'intervento di configurazione dei PC e degli strumenti di informatica individuale ed aziendale avviene solo da parte dell'Amministratore di Sistema appositamente incaricato nella procedura di gestione privacy;
- in ottica aziendale si provvede alla nomina dell'Amministratore di Sistema, che cura anche l'eventuale ripristino delle password;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche assegnate; ad ogni dipendente viene tra l'altro consegnata, nell'ambito delle procedure di trattamento dati a tutela della privacy, la policy aziendale per l'utilizzo degli strumenti aziendali;
- le risorse informatiche devono essere utilizzate esclusivamente per l'espletamento della propria attività;
- tali risorse devono essere conservate in modo appropriato; dovrà essere tempestivamente segnalato l'eventuale furto o danneggiamento;
- qualora sia previsto il coinvolgimento di soggetti terzi/*outsourcer* nella gestione dei sistemi informatici e del patrimonio informativo, tali soggetti devono impegnarsi ad operare nel rispetto della normativa vigente.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati di ASTEM SpA, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio *virus, worm, troian, spyware, dialer, keylogger, rootkit*) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, anche a mezzo di sistemi antivirus sia nel caso di attività in sede sia in caso di *smart working*;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre, o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;

- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati.

Più in particolare, i principi di sicurezza organizzativa, comportamentale e tecnologica, nonché il sistema di controllo a presidio dei descritti sistemi informatici e del patrimonio informativo di ASTEM SpA, si basa su livelli autorizzativi definiti nell'ambito di ciascuna fase operativa.

In particolare:

- la gestione delle abilitazioni deve avvenire tramite la definizione di “profili di accesso” in ragione delle funzioni svolte all'interno di ASTEM SpA;
- le variazioni al contenuto dei profili devono essere eseguite dalle funzioni deputate al presidio della sicurezza logica (Amministratore di Sistema), su richiesta delle funzioni interessate; la funzione richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative ricoperte;
- ogni utente deve essere associato ad un solo profilo abilitativo, in relazione al proprio ruolo aziendale; in caso di trasferimento o di modifica dell'attività dell'utente, deve essere riattribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato;
- le attività di implementazione e modifica dei *software*, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del *software* devono essere organizzativamente demandate a funzioni differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;
- le attività di controllo costituiscono valido presidio anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.
- è necessario svolgere adeguata formazione del personale sugli aspetti di sicurezza dei sistemi;
- è necessario provvedere alla costante predisposizione ed aggiornamento delle norme di sicurezza, al fine di garantirne nel tempo l'applicabilità, l'adeguatezza e l'efficacia;
- con specifico riferimento alla gestione di riprese ed immagini registrate a mezzo di sistemi di videosorveglianza (ad esempio, con riferimento ai parcheggi in struttura), debbono essere specificamente individuati i soggetti responsabili dell'accesso e dell'utilizzo di dette riprese ed immagini.

Tra le principali attività di prevenzione e di presidio rispetto alla commissione dei reati informatici, sono in particolare previste:

- attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti;
- pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema;
- gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità;
- prevenzione da *software* dannoso tramite opportuni strumenti e funzioni adeguate;
- formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica;

Con riferimento alla gestione degli incidenti in materia di sicurezza informatica:

- il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla tracciabilità a sistema;
- tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione;
- deve essere istituito, nell'ambito delle procedure di tutela dei dati personali, il registro *data breach*.