3

REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

ART. 24-BIS D.LGS. 231/2001.

Sommario

Art. 615-ter c.p. – 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 la reclusione fino a tre anni".*

La pena è della reclusione da uno a cinque anni:

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;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o i 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.

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».

L'oggetto giuridico tutelato dalla norma è, secondo la teoria predominante, il "domicilio informatico".

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999).

Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce o elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è "sistema informatico".

La mera copiatura dei contenuti di un sito, realizzata semplicemente dalla visualizzazione del sito senza introduzione nella "memoria interna" del sito o nei programmi che ne consentono il funzionamento, non concreta interazioni con il sistema informatico come definito dalla giurisprudenza; peraltro, si segnala che la norma in questione è stata introdotta al fine di reprimere il fenomeno degli hacker, cosa ben diversa dalla consultazione / visualizzazione / copiatura del contenuto di una pagina web.

Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico.

Sono tali quelle protezioni (che possono essere apposte sia a livello di apparecchiature (hardware) che di programmi (software) che integrano quei peculiari meccanismi operativi che impediscono un libero accesso al sistema e, quindi, la presa di cognizione di informazioni e dati ivi rinvenibili) a terzi estranei (ad esempio, codice alfanumerico di accesso, chiave di avviamento, eccetera.

L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce, infatti, l'estrinsecazione della voluntas excludendi manifestata dal titolare del relativo ius.

L'accesso ad un sistema non protetto, pertanto, risulta atipico e penalmente lecito ma non anche civilisticamente, dovendosi, a tale riguardo, ulteriormente verificare in concreto un danno ingiusto risarcibile ex articolo 2043 CC.

La Corte di Cassazione ha aderito all'orientamento interpretativo estensivo dell'art. 615-ter parte seconda e stabilito la configurabilità del reato "nel caso in cui il soggetto legittimato all'accesso per motivi di servizio o di ufficio s'introduca per motivi diversi".

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Art. 615 quater c.p. - 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.

Sanzioni pecuniarie: da € 25.800 a € 464.700

Sanzioni interdittive: da 3 a 24 mesi

Art. 615 quinquies c.p. - 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*."

Sanzioni pecuniarie: da € 25.800 a € 464.700

Sanzioni interdittive: da 3 a 24 mesi

Art. 617 - quater c.p. - 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 la reclusione da sei mesi a quattro anni.*

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. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

- 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;

- 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;

- da chi esercita anche abusivamente la professione di investigatore privato».

La norma mira a impedire l'intercettazione fraudolenta, ravvisabile ogniqualvolta l'agente prenda conoscenza delle comunicazioni in maniera occulta e senza essere legittimato.

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Art. 617-quinquies c.p. - Installazione di apparecchiature atte ad intercettare, impedire od 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 la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater».

La norma sanziona la semplice predisposizione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

L'attività illecita d'intercettazione, nel silenzio dell'art. 617- quinquies c.p., deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico qual è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso ad un sistema attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione.

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

I danneggiamenti informatici

Art. 635 c.p. - Danneggiamento

"*Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a un anno o con la multa fino a lire seicentomila.*

La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso:

1) con violenza alla persona o con minaccia;

L'art. 635-bis non si limita ad ampliare ed integrare la norma sul danneggiamento (art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilo sanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni.

Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, quali il video, la tastiera, etc.

Il danneggiamento, inoltre, può riguardare anche i dati e i programmi informatici nonché le informazioni contenute nel sistema.

L'art. 635 bis richiede che i beni informatici oggetto di aggressione siano «altrui»: il problema del significato da attribuire a tale termine sembra destinato ad assumere rilevanza pratica proprio in relazione alla nuova figura di danneggiamento informatico, stante la diffusa prassi di procurarsi la disponibilità di hardware e di software attraverso contratti di locazione (anziché di compravendita), solitamente accompagnati dalla contestuale conclusione di un contratto di assistenza e/o manutenzione con lo stesso fornitore.

Il danneggiamento si può attuare nella distruzione e nel deterioramento e nell'inservibilità totale o parziale.

Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici.

«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.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Art. 635-ter c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

«*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.*

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.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Art. 635-quater c.p. - 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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

Oltre ad essere realizzabile mediante le condotte indicate nell'art. 635-bis, è prevista anche la punibilità di chi introduce o trasmette dati, informazioni o programmi. Tale previsione si è resa necessaria per punire specificamente i danneggiamenti realizzabili anche a distanza mediante malware introdotti o fatti circolare in rete.

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Art. 635-quinquies c.p. - 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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

La semplice “condotta” diretta alla commissione del reato, con eccezione di quanto previsto dall’art. 635-bis, è di per sé già punibile non essendo necessario provare che il comportamento del reo raggiunga lo scopo prefissato, venendo quest’ultimo ad influire solo sulla quantificazione della pena.

Il legislatore anticipa la soglia di punibilità al fine di meglio sottolineare e quindi sanzionare tutta una serie di comportamenti illeciti riscontrati in questi anni.

Sanzioni pecuniarie: da € 25.800 a € 774.500

Sanzioni interdittive: da 3 a 24 mesi

Le frodi informatiche

Art. 640-ter c.p. - Frode informatica in danno dello Stato o di altro Ente Pubblico

"*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 con la reclusione da sei mesi a tre anni e con la multa da € 51 a € 1.032."*

"La pena è della reclusione da uno a cinque anni e della multa da € 309 a € 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

"La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti."

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma44 o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5,limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7.

Il delitto si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi in esso contenuti o ad esso pertinenti, un soggetto procura a sé o ad altri un ingiusto profitto arrecando altrui danno (in concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente).

Sanzioni pecuniarie: da € 25.800 a € 774.500.

Se, in seguito alla commissione del delitto, l'ente ha conseguito un profitto di rilevante gravità o è derivato un danno di particolare gravità, si applica la sanzione pecuniaria da € 51.600 a € 929.400.

Sanzioni interdittive: da 3 a 24 mesi

Art. 640 quinquies c.p - 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.

Sanzioni pecuniarie: da € 25.800 a € 619.600

Sanzioni interdittive: da 3 a 24 mesi

La falsificazione di documenti informatici

Art. 491-bis c.p. - Documenti informatici.

«*Se alcuna delle falsità previste nel presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private*».

I documenti informatici hanno la stessa rilevanza di quelli cartacei. Per "documento informatico" deve intendersi – secondo quanto espressamente indicato dall'articolo 1,lett. p) del decreto legislativo n. 82 del 7 marzo 2005 (il cd Codice dell'Amministrazione Digitale) - "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

Il capo III del c.p. (all'interno del quale si colloca l'art. 491-bis) s'intitola "Della Falsità in atti" e comprende vari reati di falso, sia in atti pubblici che privati:

476: falsità materiale commessa dal pubblico ufficiale in atti pubblici

477: falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative

478: falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e i attestati del contenuto di atti

479: falsità ideologica commessa dal pubblico ufficiale in atti pubblici

480: falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative

481: falsità ideologica in certificati commessa da persone esercenti servizio di pubblica necessità

482: falsità materiale commessa dal privato

483: falsità ideologica commessa dal privato in atto pubblico

484: falsità in registri notificazioni

487 abuso di foglio firmato in bianco da parte del pubblico ufficiale, con redazione di atto pubblico

489: uso di atto falso, senza essere concorso nella falsificazione

490: soppressione, distruzione e occultamento di atti veri

491: falsificazione di cambiale o altri titoli di credito

493 ter: indebito utilizzo falsificazione di carte di credito e di pagamento

Sanzioni pecuniarie: da € 25.800 a € 619.600

Sanzioni interdittive: da 3 a 24 mesi

Aree a rischio

I reati-presupposto sono connessi alla disponibilità di un PC e/o di accesso alle postazioni di lavoro dotate di connessione telematica alla rete aziendale e al web.

Pressoché tutti gli uffici utilizzano le tecnologie dell'informazione sicché l'area di rischio per la commissione di reati informatici corrisponde con l'intera attività aziendale, in particolare però si individua come aria preponderante di rischio l'area aziendale che specificamente si occupa della gestione dei sistemi informatici e telematici nonché delle informazioni e dei dati aziendali:

protezione dei dati e sicurezza interna;

gestione dei profili degli utenti e dei processi di autenticazione;

gestione e protezione delle postazioni di lavoro;

gestione degli accessi verso l'esterno;

gestione e protezione delle reti;

gestione degli output di sistema e dei dispositivi di memorizzazione;

sicurezza dell'hardware;

utilizzo della posta elettronica e delle reti telematiche

gestione delle autorizzazioni e delle licenze di programmi software e banche dati

monitoraggio e controllo dei software installati.

Principi di comportamento

per la prevenzione di reati informatici

Organizzazione aziendale e policies aziendali

Ai fini dell'attuazione dei comportamenti di cui sopra DPV si è dotata di apposite procedure volte ad attuare i principi di cui al Regolamento Europeo - GDPR in materia di privacy ed ha nominato un Responsabile in materia per il controllo degli adempimenti di legge e le opportune verifiche in merito alla effettiva operatività delle procedure.

Le stesse impediscono ai soggetti che utilizzano strumenti informatici l'accesso a banche dati non connesso alle effettive necessità legate alla funzione aziendale svolta.

Inoltre la Società organizza periodici corsi di formazione e aggiornamento in materia di trattamenti dei dati al fine di formare e sensibilizzare in merito all'importanza di accessi a dati e strumenti altrui solo nel rispetto dei diritti e della riservatezza altrui.

I medesimi principi sono attuati nel trattamento da parte della Società dei dati e degli strumenti in uso ai dipendenti.

DPV tramite i responsabili del settore I.T. assolve i seguenti adempimenti:

1) fornisce ai Destinatari un'adeguata informazione circa il corretto utilizzo degli user-id e delle password per accedere ai principali sottosistemi informatici utilizzati presso la Società;

2) limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi da parte dei Destinatari, permettendo la possibilità di utilizzare tali sistemi esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

3) effettua, per quanto possibile, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;

4) predispone e mantiene adeguati strumenti di salvaguardia dell'integrità fisica delle risorse informatiche della società (es. server, PC, ecc.);

5) predispone e mantiene adeguati strumenti di salvaguardia dell'integrità logica dei dati e delle informazioni gestite dalla società.

In linea generale è emersa una grande attenzione nelle procedure di protezione dei dati sensibili, migliorate ulteriormente a partire dal 2019 grazie alla delocalizzazione dei server principali che sono ora situati presso un'azienda gestita da personale altamente qualificato.

Le protezione dei dati aziendali è state ulteriormente migliorata anche sul piano operativo ossia è stato ristretto l'accesso alle singole cartelle di lavoro ai soli soggetti incaricati dello sviluppo dei progetti, rendendo così impossibile la visualizzazione di contenuti e dati che esorbitano dalla propria competenza.

Il soggetti apicali responsabili della procedura possono visionare un numero maggiore di cartelle, ma solo quelle che riguardano la propria area di competenza.

Solo l'admin di sistema, ruolo attualmente rivestito da un soggetto altamente qualificato in materia informatica, ha la possibilità di visionare i contenuti aziendali nella loro totalità e di accedere a tutte le cartelle presenti all'interno dei server: tali operazioni sono consentite esclusivamente per effettuare le procedure di aggiornamento, manutenzione e riorganizzazione dei contenuti aziendali.

In ogni caso, soggetti apicali e preposti dispongono di una propria area personale "in cloud" (nella quale possono inserire bozze di progetti o altri documenti che vogliono mantenere riservati) il cui accesso è limitato da un blocco "nome utente e password".

Inoltre vige il divieto, specificato nelle norme di regolamento aziendale a conoscenza di tutti i dipendenti e dirigenti di DPV, di collegare devices esterni ai sistemi aziendali (es. personal computer, chiavette usb, dischi di backup) e di effettuare operazioni di download su di essi.

L'area IT ha perfezionato un sistema di tracking che registra le operazioni di centinatura dei file aziendali, individuando mediante sistema di riconoscimento ID l'utente che ha effettuato l'operazione di eliminazione del dato aziendale oltre al giorno e all'ora in cui l'ha fatto.

Nel corso del 2020 sarà oggetto di discussione e confronto tra l'area IT e la dirigenza, l'introduzione di un sistema di sicurezza avanzato che impedisca a qualsiasi device esterno la possibilità di effettuare il download dei dati aziendali, andando così ad incrementare e a migliorare ulteriormente il livello di sicurezza e protezione informatica della società.

Nell'ambito della gestione dei sistemi informatici, l'attività di DPV S.p.A. è improntata a garantire, in via primaria, la riservatezza dei dati e delle informazioni, l'integrità degli stessi nonché la loro piena disponibilità da parte dei soggetti autorizzati.

DPV S.p.A., ricorrendo a consulenti esperti in materia, si è dotata di un sistema di gestione informatica idoneo a prevenire i reati previsti dalla presente sezione.

In primo luogo, è previsto un sistema di accesso alle postazioni informatiche mediante l'utilizzo di password, di almeno 8 caratteri, in dotazione ai singoli destinatari. Tali password non contengono elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né alla Società. Il destinatario sceglie autonomamente la password di accesso, che deve essere modificata ogni sei mesi, e la custodisce in busta chiusa che viene conservata nella cassaforte in un plico sigillato. È responsabilità del Titolare del trattamento provvedere alla disattivazione della password in caso di non utilizzo del computer.

Il sistema informatico di DPV S.p.A. è protetto da un adeguato antivirus che viene regolarmente aggiornato con funzione automatica e con scansione per ogni aggiornamento con cadenza almeno settimanale; sono altresì stati installati filtri antispam onde garantire una corretta ed efficace gestione della posta elettronica.

E' altresì previsto un sistema di back up giornaliero dei dati contenuti nei computers in modo da ridurre al minimo il rischio di perdita degli stessi.

Per le ulteriori, specifiche procedure, si rimanda a quanto previsto nel Documento Programmatico per la Sicurezza.

I programmi informatici che sono installati sui computers (quali ad es. Microsoft Word, Excel, Autocad) sono versioni ufficiali debitamente licenziate; le relative licenze sono correttamente archiviate, custodite e tenute a disposizione.

Qualora dovessero emergere situazioni rilevanti che compromettano l'applicazione ed attuazione del sistema, l'OdV dovrà, anche su segnalazione delle funzioni competenti, darne tempestiva comunicazione al Consiglio di Amministrazione proponendo le appropriate modifiche in ordine ad una eventuale adeguata revisione del Modello.

DIVIETI

1) alterare documenti informatici o telematici, pubblici o privati, aventi efficacia probatoria
2) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati
3) accedere abusivamente al sistema informatico o telematico della Società al fine di alterare o cancellare dati o informazioni
4) utilizzare passwords di altri utenti aziendali per accedere alle postazioni di lavoro proprie o altrui o alla rete aziendale o al Web
5) accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di soggetti abilitati
6) detenere e utilizzare abusivamente codici, psw o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate
7) detenere e utilizzare abusivamente codici, psw o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate
8) svolgere attività di approvvigionamento, produzione, diffusione di apparecchiature o software allo scopo di danneggiare un sistema informatico o telematico di soggetti pubblici o privati, le informazioni i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento
9) svolgere attività di modifica o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità
10) danneggiare informazioni, dati e programmi informatici o telematici altrui
11) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità
12) produrre e trasmettere documenti in formato elettronico con dati falsi o alterati
13) accedere a portali o banche dati di terzi qualora non si sia in legittimo possesso delle credenziali di accesso m. divulgare, cedere o condividere le proprie credenziali di accesso
14) installare software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di leggi e regolamenti
15) modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale o senza autorizzazione
16) fare copie o backup o trasferimenti in proprio favore di dati contenuti nella rete aziendale senza autorizzazione del proprio superiore gerarchico o degli organi amministrativi della società
17) acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
18) accedere da terminali, in qualsiasi modo legati all'attività lavorativa svolta per la Società, a materiale vietato dalla legge (ad es. contenuti pornografici o pedopornografici o di propaganda politica o religiosa di carattere sovversivo o eversivo) o che possa costituire pericolo per la sicurezza della rete informatica o telematica
19) acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.)

20) porre in essere, direttamente o ricorrendo a soggetti terzi, dei comportamenti come il phishing, l'hacking o la diffusione di programmi di malware finalizzati al furto e/o all'indebito utilizzo dell'identità digitale.
21) utilizzare software e/o hardware atti ad intercettare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici
22) cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti
23) distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati

OBBLIGHI

1) utilizzare le risorse informatiche software hardware esclusivamente per l'esercizio delle mansioni aziendali, astenendosi da qualsivoglia utilizzo per fini privati, e sempre in conformità con la normativa di legge e con le direttive aziendali
2) segnalare all'amministratore di rete eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni). L'amministratore di rete avrà di conseguenza l'obbligo di riferire agli amministratori della società e all'organismo di vigilanza di porre in essere tutte le accortezze tecniche tali per riparare il danno, recuperare i dati e fare le dovute segnalazioni alle autorità giudiziarie competenti nonché, nel caso di data breach che incida sui diritti di privacy di terzi, all'Autorità garante della privacy;
3) il responsabile settore informatico della società sono tenuti a dotare i sistemi informatici di adeguato software firewall e antivirus, ed ogni operatore è tenuto a non disattivarli mai se non dietro autorizzazione e con l'assistenza degli amministratori di sistema.
4) osservare la normativa a tutela della Privacy (codice privacy e G d.p.r.)
5) evitare di introdurre o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente autorizzate
6) evitare di trasferire all'esterno dell'Azienda o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie funzioni
7) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche
8) impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dall'Azienda stessa
9) provvedere alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale

Le procedure adottate da DPV S.p.A.

DPV S.p.A., al fine di garantire che i principi e le regole enunciate nel Codice Etico e nel Modello siano costantemente e correttamente attuati, si richiama ai principi già in vigore e specificamente richiamati dalla presente Sezione della Parte Speciale, nonché dalle procedure già esistenti e conformi alla disciplina normativa di settore.

Eventuali, ulteriori, specifiche procedure nella materia oggetto della presente Sezione potranno eventualmente essere adottate, se ritenuto opportuno, all'esito dell'attività di monitoraggio sullo stato di attuazione del presente Modello e/o a seguito di specifiche segnalazioni eventualmente formulate all'OdV.