Modello di organizzazione e gestione (ai sensi del D.lgs. 8 giugno 2001, n. 231)

PARTE SPECIALE B

Reati Informatici e Trattamento Illecito di Dati

Approvato dal Consiglio di Amministrazione di AS 24 ITALIA S.R.L. il 22 giugno 2021

Primo aggiornamento con delibera del CdA del 31 marzo 2025

1. FATTISPECIE DI REATO E PRINCIPI NORMATIVI

L'art. 24-bis che prevede i "*Delitti informatici e trattamento illecito di dati*" è stato introdotto dalla Legge n. 48/08, legge di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, convenzione redatta a Budapest il 23 novembre 2001.

Successivamente, l'articolo è stato modificato dall'art. 19 della L. 238/2021 ("Disposizioni per l'adeguamento alla direttiva n. 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio. Procedura di infrazione n. 2019/2033") nonché dalla Legge 90/2024 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".

Alla luce delle considerazioni svolte in Mappatura si considerano in questa sede anche i reati di cui all'art. 25 novies *Delitti in materia di violazione del diritto d'autore*.

Fondamentale per il corretto inquadramento delle fattispecie di reato contemplate dall'art. 24-bis è la definizione di sistema informatico: tale deve intendersi ogni sistema di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione di dati su supporti adeguati, per mezzo di impulsi elettronici. Si riportano, quindi, qui di seguito i riferimenti normativi e le descrizioni dei reati oggetto della presente Parte Speciale.

1.1. Reati informatici

491 bis – 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.

La norma sopra citata conferisce valenza penale alla commissione di reati di falso che si realizzino su un documento informatico; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.)

  Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.)

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.)

  Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.)

  Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.
- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.)

  Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 c.p.)

  Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.
- Falsità materiale commessa da privato (art. 482 c.p.)

Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):

  Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.
- Falsità in registri e notificazioni (art. 484 c.p.)

  Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):

  Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.
- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.)

  Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dal' articolo 487, si applicano le disposizioni sulle falsità materiali in atti pubblici.
- Uso di atto falso (art. 489 c.p.)

  Chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.
- Soppressione, distruzione e occultamento di atti veri (art. 490 c.p.)

  Chiunque in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute.
- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 c.p.)

Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.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.

La pena è della reclusione da due a dieci ~~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 minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;*
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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare 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 tre a dieci anni e da quattro a dodici anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Il reato consiste nell'introduzione abusiva con qualsiasi strumento in un sistema informatico o telematico protetto da misure di sicurezza ovvero nella permanenza contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Pare opportuno evidenziare che il delitto è procedibile d'ufficio solo qualora esso sia stato commesso nella sua forma aggravata, ovvero quando il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, da chi esercita anche abusivamente la professione di investigatore privato, con abuso della qualità di operatore del sistema, ovvero se

per commettere il fatto viene usata minaccia o violenza sulle cose o alle persone o ancora 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 ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art.615-quater c.p.)

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa comunica, consegna mette in altro modo a disposizione di altri o installa apparti, strumenti, parti di apparati o di strumenti, 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 a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma".

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.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 un anno e sei mesi a cinque 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 quattro a dieci anni se il fatto è commesso:

1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615 -ter, terzo comma;

2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

"Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti 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.

Quando ricorre taluna delle circostanze di cui all'articolo 617 -quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.

Estorsione informatica (art. 629, comma 3 c.p.)

Chiunque, mediante condotte di cui agli articoli 615 -ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.

Si tratta del chiarimento legislativo di un tema ampiamente discusso, ovvero se colui che subisce un attacco *ransomware* riveste il ruolo di vittima, trovandosi, peraltro, praticamente "costretto" a pagare una somma di denaro per cercare di scongiurare il danno che potrebbe derivare dalla definitiva perdita, nonché diffusione, dei dati sottratti.

La fattispecie sanziona, difatti, coloro che pongono in essere un attacco ad un sistema informatico aziendale altrui, minacciando – ad esempio – di distruggere o diffondere i dati ivi contenuti, a meno che non venga pagato un "riscatto".

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.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 due a sei anni.

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato.

La condotta criminosa si realizza attraverso la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione di informazioni, dati o software altrui.

Si precisa che il reato è procedibile a querela della persona offesa, mentre è procedibile d'ufficio se il fatto viene commesso nella forma aggravata di cui al secondo comma.

Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.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 di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.
La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)

La norma anticipa la tutela considerando integrato il reato da fatti diretti a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, anche qualora dalla condotta posta in essere non derivi la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, che viene considerata una mera circostanza aggravante.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

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 due a sei anni.
La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato.*

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 quater1 c.p.)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615 ter, terzo comma."

Brevi cenni sulla fattispecie

La fattispecie è un reato di pericolo, essendo irrilevante, ai fini della sua sussistenza, il danneggiamento di sistemi informatici.

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635 quinquies)

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, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto 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 minaccia o violenza ovvero se è palesemente armato;

3) 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 quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)

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.

1.2. Perimetro di sicurezza nazionale cibernetica di cui al D.L 105/2019

Art. 1 comma 11 D.L. 105/2019 (convertito in Legge dalla Legge 18 novembre 2019 n. 133)

"Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni".

Il Decreto trova la sua origine nella necessità, a fronte della realizzazione in corso di importanti e strategiche infrastrutture tecnologiche ed anche dei recenti attacchi alle reti di Paesi europei, di disporre, per le finalità di sicurezza nazionale, di un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale, disponendo altresì dei più idonei strumenti d'immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza in ambito cibernetico.

Pertanto, il nuovo testo normativo:

1. istituisce il "*Perimetro di sicurezza nazionale cibernetica*", ovvero "*uno strumento diretto ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale*";

2. prevede che il Perimetro sia composto da diversi attori, pubblici e privati, individuati sulla base di due specifici criteri ed in particolare:
   - il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
   - l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici e al cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

L'effettivo funzionamento del Perimetro di sicurezza nazionale cibernetica dipende dal decreto del Presidente del Consiglio dei Ministri del 30 luglio 2020, n. 131 pubblicato in Gazzetta Ufficiale il 21 ottobre 2020 che definisce i criteri ed individua i soggetti e i settori di attività rientranti all'interno del Perimetro di sicurezza.

L'art. 2 del suddetto D.P.C.M., individua quali soggetti che esercitano funzioni e servizi essenziali:

- i soggetti a cui l'ordinamento attribuisce compiti volti ad assicurare la continuità dell'azione di Governo e degli Organi Costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della Giustizia, la funzionalità dei sistemi economici e finanziari e dei trasporti;
- i soggetti che prestano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove pongano in essere: attività strumentali all'esercizio di funzioni essenziali per lo Stato; attività necessarie per l'esercizio e il godimento di diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Rientrano, pertanto, all'interno del Perimetro di sicurezza nazionale cibernetico i soggetti, pubblici o privati, che operano nei seguenti settori: interno; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; entri previdenziali e di lavoro; c.d. tecnologie critiche ai sensi dell'art. 4, paragrafo 1, lettera b) del Regolamento UE 2019/452 (l'intelligenza artificiale, la robotica, i semiconduttori, la cybersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie).

I soggetti pubblici e privati, che, ai sensi dell'art. 2 rientrano all'interno del Perimetro di sicurezza nazionale cibernetica vengono inseriti all'interno di una lista contenuta in un atto amministrativo adottato e periodicamente aggiornato dal Presidente del Consiglio dei Ministri su proposta del CISR.

1.3. Delitti in materia di violazione del diritto d'autore (Legge 633/1941)

Art. 171 – reati presupposto evidenziati in maiuscolo

Salvo quanto previsto dall'art. 171-bis e dall'articolo 171-ter, è punito con la multa da Euro 51 a Euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nel territorio dello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) METTE A DISPOSIZIONE DEL PUBBLICO, IMMETTENDOLA IN UN SISTEMA DI RETI TELEMATICHE, MEDIANTE CONNESSIONI DI QUALSIASI GENERE, UN'OPERA DELL'INGEGNO PROTETTA, O PARTE DI ESSA;

b) rappresenta, esegue o recita in pubblico o diffonde con o senza variazioni od aggiunte, una opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di produrre o di rappresentare;

e) (Omissis);

f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

Chiunque commette la violazione di cui al primo comma, lettera a-bis), e' ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

LA PENA È DELLA RECLUSIONE FINO AD UN ANNO O DELLA MULTA NON INFERIORE AD EURO 516 SE I REATI DI CUI SOPRA SONO COMMESSI SOPRA UN'OPERA ALTRUI NON DESTINATA ALLA PUBBLICAZIONE, OVVERO CON USURPAZIONE DELLA PATERNITÀ DELL'OPERA, OVVERO CON DEFORMAZIONE, MUTILAZIONE O ALTRA MODIFICAZIONE DELL'OPERA MEDESIMA, QUALORA NE RISULTI OFFESA ALL'ONORE OD ALLA REPUTAZIONE DELL'AUTORE. La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da Eur 1.032 a Euro 5.164.

Art. 171 bis

Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati ai sensi della legge, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da Euro 2.582 ad Euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a Euro 15.493 se il fatto è di rilevante gravità.

Chiunque, al fine di trarne profitto, su supporti non contrassegnati ai sensi della legge riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da Euro 2.582 ad Euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa ad E uro 15.493 se il fatto è di rilevante gravità.

Art. 171 ter

E' punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da Euro 2.582 ad Euro 15.493 chiunque ai fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente

fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta l'apposizione di contrassegno ai sensi della presente legge, privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale.

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

2. È punito con la reclusione da uno a quattro anni e con la multa da Euro 2.582 ad Euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma l;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;

e) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

Art. 171 septies

La pena di cui all'articolo 171-ter, comma 1, si applica anche:

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

Art. 171 octies

Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da Euro 2.582ad Euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio. La pena non è inferiore a due anni di reclusione e la multa ad Euro 15.493 se il fatto è di rilevante gravità.

2. PROCESSI SENSIBILI

La Società ha ritenuto opportuno indicare le misure adottate al fine di scongiurare il verificarsi di comportamenti illeciti connessi alla disponibilità di mezzi informatici, in quanto la sicurezza dei sistemi informatici è ritenuta elemento essenziale del sistema di controllo aziendale.

Oltre al reato di frode informatica di cui all'art. 640 ter c.p., già considerato nella Parte Speciale A), il legislatore ha inserito ulteriori ipotesi delittuose che rilevano ai fini della presente Parte Speciale nei limiti in cui siano commesse nell'interesse o a vantaggio della Società.

L'ipotesi che la commissione di talune fattispecie integri il suddetto requisito è un rischio alquanto marginale, ma si è ritenuto opportuno inserire una Parte Speciale *ad hoc* in ragione del fatto che il sistema informatico prevede la gestione di tutti i dati aziendali ed occorre, pertanto, un corretto utilizzo dello stesso.

AS 24 ITALIA utilizza un sistema informatico di tipo tradizionale basato su un'architettura client – server che consente di gestire i processi registrando le operazioni in tempo reale, permettendo la tracciabilità e l'identificazione degli autori.

In ragione dell'attività svolta dalla Società possono ritenersi esclusi i rischi connessi ai seguenti reati presupposto:

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p);
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Estorsione informatica (art. 629, comma 3 c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 quater1 c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblico interesse ~~a utilità~~ (art. 635-quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);
- Art. 171 ter;
- Art. 171 septies;
- Art. 171 octies.

Infine, in relazione alle "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*", la Società, allo stato, non ritiene di poter essere inserita tra i soggetti obbligati allo scambio di informazioni previste in tema di sicurezza nazionale cibernetica.

Per le restanti categorie di reato si ritiene che i rischi, seppur astratti, siano propri di ogni ambito aziendale che utilizza le tecnologie informatiche.

I reati sopra considerati hanno, infatti, come presupposto la disponibilità di un terminale e di un accesso alle postazioni di lavoro; per tale ragione le aree di attività ritenute più specificamente a rischio sono quelle che comportano l'utilizzo di un personal computer, l'accesso alla posta elettronica, l'utilizzo di programmi informatici e l'accesso a internet.

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati nella presente Parte Speciale, sono, quindi, collegate a tutte le attività di gestione e utilizzo dei sistemi informatici e delle informazioni aziendali (c.d. patrimonio informativo), nell'ambito della quale sono ricomprese le attività di:

- gestione del profilo utente e del processo di autenticazione;
- gestione e protezione della postazione di lavoro;
- gestione degli accessi verso l'esterno;
- gestione e protezione delle reti;
- sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.) dei sistemi informatici.

È possibile, inoltre, ravvisare attività sensibili nella gestione delle autorizzazioni e delle licenze di programmi software e banche dati.

3. PRINCIPI GENERALI DI COMPORTAMENTO

Ai fini della prevenzione dei reati presi in considerazione dalla presente Parte Speciale, è, in primo luogo, fatto divieto ai destinatari di porre in essere, o concorrere in qualsiasi forma, nella realizzazione di comportamenti tali da integrare le fattispecie sopra elencate.

In ogni caso, AS 24 ITALIA pone a carico dei destinatari l'espresso divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;
- 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 altri soggetti abilitati;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/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;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- 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;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati.

Inoltre, è richiesto ai destinatari di attenersi ai seguenti obblighi:

a) comportarsi in conformità alle norme di legge, di regolamento, alle procedure aziendali esistenti in ogni attività che comportino l'utilizzo di un terminale e l'accesso a sistemi informatici. Ogni soggetto che opera all'interno di AS 24 ITALIA è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (ad esempio personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività e non possono essere cedute a terzi. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;

b) ogni dipendente è tenuto alla segnalazione alla funzione RETE & CONTRATTI di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;

c) osservare rigorosamente tutte le norme poste dalla legge a tutela della Privacy;

d) garantire ed agevolare ogni forma di controllo, svolta nel rispetto dell'art. 4 dello Statuto dei Lavoratori, diretta a impedire la commissione di fattispecie delittuose;

e) evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo quanto acquisito con il consenso di questi ultimi, nonché applicazioni/software che non siano state preventivamente autorizzate;

f) evitare di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell'Azienda stessa o del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

g) evitare l'utilizzo di *passwords* di altri utenti aziendali, salvo espressa autorizzazione ricevuta in tal senso e connessa a impellenti esigenze di lavoro;

h) evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

i) utilizzare la connessione a Internet per gli scopi e per il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento. Non è consentito

accedere, attraverso terminali in qualsiasi modo legati a AS 24 ITALIA, a siti e pagine web contenenti materiale vietato dalla legge (ad es. pedopornografici) o che possano costituire pericolo per la sicurezza della rete informatica;

j) impiegare sulle apparecchiature dell'Azienda solo prodotti ufficialmente acquisiti dalla stessa;

k) astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

l) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

m) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'Azienda;

n) osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

I responsabili delle funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

4. PROCEDURE DA APPLICARE NEI PROCESSI SENSIBILI

La Società si è dotata di adeguate soluzioni di sicurezza, alcune in conformità alle disposizioni in materia di tutela dei dati personali, per prevenire e controllare i rischi in tema di tecnologia dell'informazione, a tutela del proprio patrimonio informativo e dei dati personali dei soggetti interessati.

Si riporta tabella riassuntiva delle principali misure di sicurezza informatiche

Misure	**Descrizione**	**Rischi contrastati**
Sistema di autenticazione con credenziali personali	AS 24 ITALIA utilizza come sistema di accesso per l'utilizzazione dei personal computer, l'autenticazione tramite credenziali personali (username, password).	Sottrazione di credenziali di autenticazione
Antivirus	È stato adottato un sistema antivirus con scansione in tempo reale, installato su tutti gli strumenti elettronici in dotazione.	Azione di virus o di programmi suscettibili di recare danno

Piano di back up dei dati	Il Piano di back up dei dati è gestito direttamente da AS 24 SOCIETÈ SEMPLIFIEE PAR ACTIONES.	Azione di virus o di programmi suscettibili di recare danno
Firewall	La gestione dei Firewall e delle relative politiche è di competenza e gestione di AS 24 SOCIETÈ SEMPLIFIEE PAR ACTIONES	Accessi esterni non autorizzati

Per quanto riguarda le attività di lavoro svolte in modalità Smart Working il Gruppo ha predisposto specifiche procedure e/o guide relative alla gestione delle risorse informatiche e di comunicazione, in particolare volte a garantire la sicurezza delle informazioni e l'applicazione delle regole da parte di tutti i dipendenti (utilizzatori) delle pratiche aziendali in materia.

5. IL SISTEMA DI CONTROLLO: COMPITI E POTERI DELL'ORGANISMO DI VIGILANZA

Il sistema di controllo predisposto da AS 24 ITALIA prevede la supervisione ad opera dell'Organismo di Vigilanza, soggetto istituzionalmente preposto alla verifica dell'idoneità ed efficacia del modello.
L'OdV, pertanto, effettua periodicamente specifici controlli sulle attività connesse ai "processi sensibili" al fine di verificare il rispetto dei Principi Generali di comportamento e delle procedure e delle istruzioni operative come sopra indicate.
È stata all'uopo redatta specifica parte speciale che regolamenta i flussi informativi nei confronti dell'OdV, al fine di fornire allo stesso le informazioni necessarie per l'espletamento dell'attività di verifica e controllo (Parte Speciale Z "Flussi informativi nei confronti dell'OdV").
In ogni caso all'OdV sono garantiti autonomi poteri di iniziativa e controllo e potrà avere accesso in qualunque momento a tutta la documentazione aziendale ritenuta rilevante.
Nell'ambito dei propri poteri potrà indire, a sua discrezione, riunioni specifiche con i soggetti deputati alla gestione dei "processi sensibili" e potrà attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello.

6. SISTEMA DISCIPLINARE

L'inosservanza dei principi e delle procedure previste nella presente parte speciale è passibile di sanzione disciplinare secondo quanto indicato nella Parte Generale alla sezione "Sistema disciplinare".