PARTE SPECIALE “I”

DELITTI INFORMATICI E DEL TRATTAMENTO ILLECITO DEI DATI

INDICE

1. *Le fattispecie dei delitti informatici*

La presente Parte Speciale è dedicata ai reati informatici previsti dall'art. 24-*bis* del Decreto, introdotto dall'art. 7 della legge 18 marzo 2008, n. 48. Si tratta di reati commessi mediante l'impiego di tecnologie informatiche o telematiche e caratterizzati da diverse tipologie di condotta.

Alcuni di questi reati sono connotati dall'uso illegittimo degli strumenti informatici e finalizzati all'accesso abusivo in un sistema informatico, alla modifica o al danneggiamento dei dati ivi contenuti, ovvero al danneggiamento del medesimo. Altri riguardano condotte di intercettazione illegittima di comunicazioni informatiche o telematiche. Infine, è prevista la fattispecie di frode informatica del soggetto certificatore della firma elettronica.

Si segnala che, ai fini penali, la legge parifica il documento informatico pubblico all'atto pubblico scritto e quello privato alla scrittura privata cartacea.

La presente parte speciale è stata di recente innovata con l'introduzione, nel sistema legislativo italiano, della Legge n. 90/2024 recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici c.d. Legge sulla Cybersicurezza*".

La legge ha come obiettivo primario l'armonizzazione della *cybersecurity* soprattutto con riferimento alla gestione degli attacchi informatici da parte delle pubbliche amministrazioni.

Nello specifico, la legge impone ai destinatari della norma l'adempimento di quattro requisiti:

-dotare l'amministrazione di una struttura per la *cybersicurezza*;

-individuare la figura del referente per la *cybersicurezza*;

-segnalare compiutamente le anomalie e/o gli incidenti informatici nelle tempistiche richieste dalla Legge;

- provvedere senza ritardo alla risoluzione della problematicità riscontrata come richiesto dai protocolli dell'Agenzia per la Cybersicurezza Nazionale.

Difatti, al fine di rafforzare i presidi in materia di *cybersecurity*, è stata emanata la direttiva c.d. "Nis 2", attraverso la quale l'Unione Europea ha imposto agli Stati membri di definire delle efficaci strategie nazionali di cybersicurezza: obiettivo primario della direttiva è cercare di reprimere gli incidenti e le minacce informatiche e, al contempo, rafforzare le barriere della sicurezza informativa comunitaria e nazionale.

Recentemente è stata innovata la materia dei "Delitti informatici e trattamento illecito dei dati", a seguito della definitiva introduzione della Legge sull'Intelligenza artificiale all'interno dell'ordinamento italiano.

Difatti, è stata pubblicata in Gazzetta Ufficiale la Legge n. 132 del 23 settembre 2025, recante "*Disposizioni e deleghe al Governo in materia di Intelligenza Artificiale*".

Il provvedimento, in linea con il cosiddetto "AI Act" (Regolamento UE 2024/1689), promuove un utilizzo corretto, trasparente e responsabile dell'Intelligenza Artificiale, introducendo il primo quadro normativo organico a livello nazionale in materia. Tra i principali obiettivi cui mira la normativa di nuovo conio, preme rammentare quelli di:

- stabilire principi di utilizzo etico, trasparente e sicuro dell'IA;
- istituire una *governance* nazionale, affidata all'AgID e all'ACN, con una Strategia nazionale coordinata dalla Presidenza del Consiglio;
- prevedere interventi specifici nei settori pubblico, sanitario, professionale e giudiziario;
- introdurre nuove fattispecie di reato legate all'uso illecito dell'IA, nonché aggravanti specifiche nel codice penale;
- delegare infine il Governo all'emanazione di decreti legislativi in materia di dati, algoritmi e responsabilità, al fine di adeguare l'ordinamento interno alle evoluzioni normative europee.

Inoltre, la legge n. 132/2025 inserisce all'interno del quadro normativo italiano la c.d. "colpa artificiale" ossia la possibilità per l'ente di rispondere nelle ipotesi di danni o reati originati dal

malfunzionamento o da errori provocati dagli algoritmi aziendali. Pertanto, alla luce della nuova disciplina, è doveroso costruire un sistema di gestione integrato di *governance* in cui interagiscano e cooperino competenze giuridiche, organizzative e tecniche.

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 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 il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare 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 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".

L'articolo offre una tutela ampia, comprensiva e anticipata che si sostanzia nel c.d. "*ius excludendi alios*", avente a oggetto tutti i dati raccolti nei sistemi informatici protetti, indipendentemente dal loro contenuto, purché attinenti alla sfera di pensiero o alle attività, lavorative e non, dell'utente, in modo da assicurare una protezione da qualsiasi tipo di intrusione che possa avere anche ricadute economico-patrimoniali.

Per sistema informatico a mente della Convenzione di Budapest del 23 novembre 2001 si intende qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base a un programma, compiono l'elaborazione automatica dei dati.

Il delitto di cui all'art. 615-*ter* c.p. integra un reato di mera condotta che si perfeziona con la violazione del domicilio informatico, mediante l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi un'effettiva lesione della riservatezza degli utenti.

Le condotte punite dal primo comma consistono: a) nell'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (da intendere come accesso alla conoscenza di dati o informazioni contenuti nel sistema, effettuato sia da lontano, sia da vicino); b) nel mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione (da intendersi come il fatto di chi persista nella già avvenuta introduzione, inizialmente autorizzata o casuale, continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema).

Secondo la giurisprudenza di legittimità quel che rileva è il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che non può considerarsi autorizzato ad accedervi e a permanervi, sia quando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema (prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro), sia quando ponga in essere

operazioni di natura diversa da quelle di cui egli è incaricato e in relazione alle quali l'accesso gli è consentito.
L'articolo pertanto punisce a titolo di dolo generico le condotte non solo di chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, ma anche di chi vi si trattiene contro la volontà, espressa o tacita, del titolare che ha il diritto di escluderlo.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)
"Chiunque, al fine di procurare a sè 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 5.164 euro. La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater". 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".

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche (art. 617 bis c.p.)
La norma prevede che "*Chiunque, fuori dei casi consentiti dalla legge, al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti idonei intercettare, impedire od interrompere comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni.*
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 uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni".
La previsione normativa è posta a tutela del bene giuridico della inviolabilità delle comunicazioni a distanza intercorrenti tra due o più soggetti.
Si tratta di una disposizione che persegue fatti prodromici alla commissione del delitto di cui all'articolo 617 c.p., al contempo, indicando infatti come condotta penalmente rilevante l'installazione di apparecchiature atte a captare o impedire comunicazioni telefoniche o telegrafiche altrui.
Il secondo comma prevede una circostanza aggravante specifica, ogni qualvolta il fatto sia commesso da determinati soggetti qualificati: un pubblico ufficiale con abuso dei propri poteri, un incaricato di pubblico servizio o un investigatore privato, o in danno di un pubblico ufficiale nell'esercizio delle sue funzioni o a causa delle funzioni stesse.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
La fattispecie prevede che *"Chiunque fraudolentemente intercetta comunicazioni relative a 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, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema".
La norma è indirizzata all'impedimento dell'intercettazione fraudolenta, che si verifica quando si prende conoscenza di comunicazioni altrui, in modo occulto e senza autorizzazione. Si tratta di una fattispecie a dolo generico e, salvo le aggravanti previste dal quarto comma, il reato è procedibile a querela della persona offesa.
In particolare, l'intercettazione si ha quando il messaggio giunge integralmente al destinatario, l'interruzione quando l'invio del messaggio viene interrotto e, pertanto, non giunge al destinatario, l'impedimento quando il messaggio non riesce nemmeno a partire.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
L'articolo dispone che: *"Chiunque, fuori dei 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 a intercettare, impedire o interrompere comunicazioni relative a 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".
La norma offre una forma di tutela anticipata rispetto a quella prevista dall'art. 617-*quater*, punendo comportamenti prodromici alle condotte descritte nel precedente articolo. Per la realizzazione della fattispecie è sufficiente il mero pericolo di arrecare danno alla libertà di comunicare e alla riservatezza.
Le condotte consistono nella installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, a nulla rilevando l'effettivo funzionamento delle stesse.

Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617 sexies c.p.)
L'articolo in esame punisce "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.*
La pena è della reclusione da tre a otto anni nei casi previsti dal quarto comma dell'articolo 617 quater. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa".
La norma in esame ha come obiettivo la tutela della veridicità ed inviolabilità delle comunicazioni a distanza tra due o più soggetti.
Il legislatore intende punire la condotta propria della falsificazione del contenuto di comunicazioni relative ad un sistema informatico o tra sistemi telematici, oppure nell'atto di formare falsamente il contenuto della comunicazione stessa, al fine di procurare un vantaggio o di arrecare ad altri un danno.
È un reato proprio, in quanto può essere commesso solamente da chi abbia un obbligo di formare o di trasmettere ad altri il contenuto di comunicazioni altrui, avendo, per ragioni del suo ufficio o della sua professione, l'autorizzazione a captare tale forma di comunicazione.
Il secondo comma prevede non un reato proprio, bensì una circostanza aggravante specifica, qualora il fatto sia commesso in danno di un sistema informatico dello Stato, oppure sia commesso

da un pubblico ufficiale con abuso dei poteri o con abuso della qualità di operatore del sistema, o se commesso da chi eserciti, anche abusivamente, la professione di investigatore privato.

Estorsione (art. 629, comma 3 c.p.)
La norma punisce "*Chiunque, mediante le 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".*
Il legislatore ha di recente modificato l'art. 24 bis con l'emanazione della Legge n. 90/2024 recante "*Disposizioni per il rafforzamento di cybersicurezza nazionale e reati informatici*".
Il nuovo comma 1 bis contempla un'ulteriore fattispecie criminosa, nel caso di specie "l'estorsione mediante attacco informatico", attraverso cui si intende promuovere il coordinamento tra il settore pubblico e privato nella creazione di programmi di formazioni specialistici per i destinatari del settore, al fine di rafforzare la protezione dei dati, le funzioni dell'Agenzia per la cybersicurezza nazionale e contrastare gli attacchi informatici.
Inoltre, la legge in oggetto mira a promuovere nuove e differenti misure per la sicurezza delle banche dati giudiziarie attraverso l'introduzione negli appalti pubblici di criteri di cybersicurezza ad hoc.
Infine, la norma punisce la condotta di chi costringe taluno a fare o ad omettere qualsivoglia cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, mediante le condotte indicate dal comma 1 dell'art. 24-bis del Decreto 231

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
Ai sensi della norma in commento *"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 fattispecie si differenzia rispetto al danneggiamento ordinario per gli interessi tutelati inerenti la realtà informatica e telematica.
Le condotte sono rappresentante dalla distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi altrui.
La condotta della "cancellazione", secondo la giurisprudenza di legittimità, deve essere interpretata nella accezione informatica e non semantica del termine, ossia come la "rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via 'definitiva' mediante il successivo svuotamento dello stesso". Pertanto, del tutto irrilevante, ai fini della sussistenza del reato, è il fatto che i file cancellati possano essere recuperati *ex post* attraverso una specifica procedura tecnico-informatica.
Secondo tale impostazione, la configurabilità del reato di danneggiamento informatico non viene dunque preclusa dall'eventuale reversibilità del danno, ritenendosi sufficiente che il bene tutelato sia stato - anche solo temporaneamente - oggetto di manomissione o alterazione rimediabile attraverso un postumo intervento riparatorio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
Ai sensi dell'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 punisce i medesimi fatti sanzionati dall'art. 635 *bis* allorquando l'attività si diriga avverso informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità.
Il bene giuridico tutelato è il patrimonio informatico in relazione alle informazioni, dati e programmi informatici statali.
Il Legislatore ha previsto al secondo comma un aggravante specifica qualora il fatto sia commesso con violenza o minaccia oppure abusando della qualifica di operatore informatico.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
L'articolo dispone: "S*alvo 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".
La fattispecie richiama le condotte di cui all'art. 635-*bis* c.p. e punisce condotte ulteriori, quali l'introduzione o la trasmissione di dati, informazioni o programmi, che danneggino, distruggano, rendano anche in parte inservibili o ostacolino il funzionamento di altrui sistemi informatici o telematici.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 quater.1)
La fattispecie in esame punisce "*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".
La fattispecie in esame è stata di recente inserita all'interno del catalogo dei reati presupposto dalla Legge n. 90/2024.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
Ai sensi della norma in commento: "*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".
L'articolo punisce le condotte dell'art. 635 *quater* dirette a sistemi informatici o telematici di pubblica utilità.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.)
L'articolo dispone: *"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."*
L'articolo tutela l'attività di rilascio di un certificato qualificato rispetto ad attività poste in essere dal certificatore che per fini ed interessi di tipo privato viola gli obblighi previsti dalla legge.
La fattispecie richiede il dolo specifico rappresentato dal fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno.

Documenti informatici (art. 491-bis c.p.)
L'articolo prevede *"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."*
Lo scopo della norma è la tutela della fede pubblica attraverso la salvaguardia dell'integrità del documento informatico nella sua valenza probatoria.

Delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105
Il comma 11 dell'articolo summenzionato prevede che *«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 cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote».*
Il decreto è volto ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.
La nuova normativa, in particolare quanto statuito dal comma 11, articolo 1, della legge in commento definisce le modalità di individuazione dei soggetti pubblici e privati che ne fanno parte,

nonché delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica ed istituisce un meccanismo teso ad assicurare dei presidi più sicuri per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi di information and communication technology (ICT) destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti.

Trattamento sanzionatorio per le fattispecie di cui all'art. 24-bis del Decreto

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 duecento a settecento quote.

1-bis. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 635-quater.1 del codice penale, si applica all'ente la sanzione pecuniaria sino a quattrocento 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, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, 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 il delitto indicato nel comma 1-bis si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni)).

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).

2. *Le "attività sensibili" ai fini del d.lgs. n. 231/2001*

L'art. 6, comma 2, lett. a) del d.lgs. n. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal d.lgs. n. 231/2001.

L'analisi dei processi aziendali di Geolog S.r.l., svolta nel corso del progetto ha consentito di individuare le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate nel paragrafo 1. Qui di seguito sono elencate le attività sensibili esaminate:

Gestione dei sistemi IT

Si tratta delle attività di gestione dei profili utente e del processo di autenticazione, gestione del processo di creazione/trattamento/archiviazione di documenti elettronici, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno, gestione e protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione, la sicurezza fisica (cablaggi, dispositivi di rete, ecc.) nonché della gestione dei software e/o banche dati protetti da licenza.

3. *Presidi di controllo*

I presidi di controllo generali che la Società ha deciso di adottare al fine di prevenire il c.d. "rischio reato" nelle attività sensibili perseguite – ovvero quelle nel cui ambito è effettivamente sussistente il rischio di commissione delle fattispecie delittuose – sono molteplici ed elencati di seguito:

1) Codice Etico;
2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;
3) diffusione del Modello tra le risorse aziendali, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet della Società;
4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito intranet della Società o messa a disposizione in formato cartaceo o telematico;
5) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari (ad es., fornitori, consulenti, appaltatori), si impegnano a rispettare le previsioni del Decreto;
6) Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi;
7) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della Società, di impegno al rispetto dello stesso, incluso il Codice Etico;
8) implementazione di un sistema di dichiarazioni periodiche (almeno semestrali) da parte dei Responsabili Interni con le quali si fornisce evidenza del rispetto e/o della inosservanza del Modello (o, ancora di circostanze che possono influire sull'adeguatezza ed effettività del Modello);
9) ove necessario, documentazione scritta, tracciabilità ed archiviazione dei contatti con la PA;
10) creazione di una "Sezione 231" all'interno della intranet aziendale, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello della Società (ad es., Modello, Codice Etico, Protocolli aziendali in esso richiamati).

La Società, inoltre, ha predisposto delle linee guida da seguire nell'adozioni dei comportamenti idonei a prevenire il rischio reato attraverso degli *standard* basilari:

- **Procedure**: gli *standard* si fondano sull'esistenza di disposizioni aziendali e/o di procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Tracciabilità**: gli *standard* si fondano sul principio secondo cui: i) ogni operazione relativa all'attività sensibile sia, ove possibile, adeguatamente registrata; ii) il processo di decisione, autorizzazione e svolgimento dell'attività sensibile sia verificabile ex post, anche tramite appositi supporti documentali; iii) in ogni caso, sia disciplinata in dettaglio la possibilità di cancellare o distruggere le registrazioni effettuate.
- **Segregazione dei compiti**: gli *standard* si fondano sulla separazione delle attività tra chi autorizza, chi esegue e chi controlla.
- **Procure e deleghe**: gli *standard* si fondano sul principio secondo il quale i poteri autorizzativi e di firma assegnati debbano essere: i) coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, indicazione delle soglie di approvazione delle spese; ii) chiaramente definiti e conosciuti all'interno della Società. Devono essere definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese.

3.1 Presidi di controllo specifici e connesse procedure con riferimento ad ogni singola attività sensibile.

Come evidenziato nel paragrafo precedente, all'esito della fase di "*risk assessment"* sono state individuate le c.d. attività sensibili alle quali discendono i presidi di controllo specifici in relazione a singole attività o categorie di attività sensibili:

Attività n. 1 Gestione dei sistemi IT (cfr. procedura omonima)

- gestione della sicurezza informatica sia a livello fisico che logico;
- gestione della attività di manutenzione dei sistemi esistenti e gestione dell'attività di elaborazione dati;
- gestione e protezione delle reti e dei dati;
- chiara segregazione di funzioni e di responsabilità nelle attività relative alla gestione della rete, alla amministrazione dei sistemi e allo sviluppo/manutenzione degli applicativi;
- gestione delle credenziali di accesso ai sistemi e loro monitoraggio periodico;
- restrizione e profilazione degli accessi a sistema mediante assegnazione di *user id* personale e *password*;
- associazione ad ogni profilo dei diritti di accesso a dati e informazioni che rientrano nelle competenze assegnate;
- rimozione delle utenze al termine del rapporto di lavoro.

N.B: Con riferimento alla presente parte speciale, la Società ha adottato una procedura *ad hoc* atta a definire con precisione i comportamenti che i soggetti responsabili devono porre in essere al fine di prevenire la commissione di uno dei reati-presupposto interessati.

Inoltre, la Società ha predisposto – a supporto di ogni singola procedura – una scheda di mappatura della suddetta attività sensibile, alla quale si rimanda integralmente.