PARTE SPECIALE B)

REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Revisione	Data	Verifica	Approvazione	Note
0	16/02/2024	C.d.A.	C.d.A.	Prima emissione

INDICE

B.1. I REATI DI CUI ALL'ARTICOLO 24-BIS DEL D.LGS. N. 231/2001. POSSIBILI MODALITÀ DI COMMISSIONE

Si riporta di seguito una sintetica descrizione dei reati richiamati nell'art. 24-*bis* del Decreto, nonché una breve esposizione delle possibili modalità di attuazione dei reati, fermo restando che, ai sensi dell'art. 26 del Decreto, la Fondazione potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

- Accesso abusivo ad un sistema telematico od informatico (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 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 di 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 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 ad otto 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 potrebbe verificarsi laddove soggetti che ricoprono posizioni apicali all'interno della Fondazione si introducano abusivamente all'interno di un sistema informatico di altra società allo scopo di carpirne segreti aziendali o elenchi di clientela, ovvero tale condotta sia perpetrata da dipendenti o collaboratori esterni sottoposti alla vigilanza e direzione dei soggetti in posizione apicale della Fondazione, qualora il reato sia commesso nell'interesse o a vantaggio di quest'ultima e la commissione di esso sia stata possibile dall'inosservanza degli obblighi di vigilanza e direzione.

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

"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'acceso 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 fino ad un anno e con la multa fino ad euro 5.164,00.

La pena è della reclusione da uno a due anni e della multa da euro 5.164,00 a euro 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater c.p.".

A titolo di esempio, si fa menzione della condotta di soggetti apicali della Fondazione i quali abusivamente si procurino numeri seriali di apparecchi cellulari appartenenti ad altri soggetti, poiché, attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta clonazione), è possibile realizzare un'illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche.

Si espone, altresì, il caso in cui un soggetto che ricopre una posizione apicale all'interno della Fondazione ovvero un soggetto ad esso sottoposto si procuri il codice di accesso alla home banking di terzi al fine di effettuare transazioni bancarie favorevoli alla Fondazione.

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615 quinquies c.p.)

"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 10.329,00".

A titolo di esempio, si menziona il caso in cui un soggetto posto in posizione apicale della Fondazione si procuri un programma informatico utilizzabile al fine di danneggiare il sistema informatico di un'altra fondazione, ovvero tale condotta sia perpetrata da dipendenti o dai collaboratori sottoposti alla vigilanza e direzione dei soggetti in posizione apicale della Fondazione, qualora il reato sia commesso nell'interesse o a vantaggio di quest'ultima e la commissione di esso sia stata possibile dall'inosservanza degli obblighi di vigilanza e direzione.

- 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 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 al primo e secondo comma sono puniti 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:
1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
3) da chi esercita anche abusivamente la professione di investigatore privato".

A titolo di esempio, si indica il caso in cui un dipendente, un collaboratore o soggetto apicale della Fondazione intercetti la corrispondenza via e-mail di un'altra fondazione ITS.

- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

"*Chiunque, fuori dei 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".*

A titolo esemplificativo, si indica il caso in cui dipendenti, collaboratori e/o soggetti apicali della Fondazione installino abusivamente apparecchiature atte ad intercettare comunicazioni relative ad un sistema informatico di un'altra fondazione ITS.

- 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 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".

A titolo esemplificativo, si indica il caso in cui un soggetto in posizione apicale distrugga informazioni o dati informatici di un dipendente o di un collaboratore sgradito ai vertici della Fondazione e/o non idoneo allo svolgimento delle mansioni affidategli, allo scopo di precostituire delle cause di addebito disciplinare.

- 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.)

"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."

A titolo di esempio, si menziona il caso del dipendente, del collaboratore o del soggetto apicale della Fondazione che tenti di alterare il sistema informatico del MIUR; della Agenzia delle Entrate, INPS o di altro ente pubblico.

- 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 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."

A titolo di esempio, si indica il caso in cui, attraverso l'invio di un messaggio di posta elettronica contenente in allegato un documento affetto da un virus, un soggetto apicale della Fondazione, un suo collaboratore e/o un suo dipendente renda in tutto o in parte inservibile la rete informatica di un'altra fondazione ITS.

- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635 quinquies c.p.)

"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".

A titolo di esempio, si indica il caso in cui, attraverso l'invio di un messaggio di posta elettronica contenente in allegato un documento affetto da un virus, un soggetto apicale della Fondazione, un suo collaboratore e/o un suo dipendente tenti di rendere inservibile la rete informatica del MIUR, dell'Agenzia delle Entrate o di altro ente pubblico, acquisendo informazioni memorizzate su supporto informatico, da cui possano scaturire rilievi di responsabilità a carico della Fondazione o dei suoi dipendenti o dei suoi collaboratori.

- 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 51,00 a 1.032,00 euro".

A titolo di esempio, si indica il caso in cui un soggetto apicale della Fondazione istighi il soggetto che presta servizio di certificazione di firma elettronica per la fondazione a violare gli obblighi di legge per il rilascio di un certificato qualificato al fine di conseguire un ingiusto profitto.

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

"Se alcune delle falsità previste dal 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".

A titolo di esempio, si cita il caso di un soggetto in posizione apicale o di un collaboratore che falsifichi un contratto, formatosi anche attraverso uno scambio di e-mail, nell'interesse o a vantaggio della Fondazione.

B.2. AREE POTENZIALMENTE 'A RISCHIO'. ATTIVITÀ 'SENSIBILI'. REATI PROSPETTABILI E PRINCIPI GENERALI DI COMPORTAMENTO

In relazione all'attività svolta dalla Fondazione, le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati di cui al precedente punto, le attività "sensibili" e le funzioni/unità organizzative in essere presso la Fondazione come previsto nelle procedure in vigore:

1) ***Gestione dei sistemi informativi e della sicurezza informatica:*** riguarda le attività di gestione dei profili utente e del processo di autenticazione, gestione del processo di creazione/trattamento/archiviazione di documenti elettronici con valore probatorio, 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.

Risulteranno, quindi, particolarmente a rischio tutte le attività attuate per il tramite di elaboratori elettronici. Si indicano, a titolo esemplificativo:

- la gestione integrale dei sistemi informativi interni e, in ogni caso, l'attività di installazione, manutenzione, programmazione e collegamento in rete dell'hardware della Fondazione;
- l'attività di creazione, gestione ed aggiornamento del software interno;
- la corrispondenza, a mezzo di posta elettronica, con clienti, finanziatori, soggetti partner, fornitori, uffici ed enti pubblici;
- la corrispondenza, sempre a mezzo di posta elettronica, con enti, altre ITS Academy o di diversa natura;
- la circolazione delle e-mail interna alla Fondazione;
- i rapporti con i soggetti che prestano il servizio di certificazione di firma elettronica;
- la gestione accessi, account, profili e adempimenti telematici;
- i rapporti con eventuali consulenti informatici esterni;
- le operazioni di home banking;
- i rapporti con la CCIAA.

La regolamentazione delle attività deve prevedere:

- **Segregazione delle attività:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, esegue e controlla;

- **Esistenza di procedure/norme/circolari**: devono esistere disposizioni interne, procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- **Poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono essere coerenti con le responsabilità assegnate, prevedendo ove richiesto delle soglie di approvazione delle spese; inoltre devono essere chiaramente definiti e conosciuti all'interno della Fondazione
- **Tracciabilità:** ogni operazione relativa all'attività sensibile, deve essere adeguatamente registrata. Il processo di autorizzazione, di svolgimento e di controllo deve essere verificato ex-post tramite appositi supporti documentali.

Nell'espletamento di tutte le operazioni compiute con i mezzi informatici e/o telematici, oltre alle regole di cui al presente Modello, gli Aderenti (fondatori e partecipanti), i dipendenti e i lavoratori autonomi che prestano la loro opera in favore della Fondazione (ed i consulenti, nella misura necessaria alle funzioni dagli stessi svolte) devono conoscere e rispettare:

- le procedure interne, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale, interne ed organizzativa della fondazione ed i compiti attribuiti;
- il Codice Etico;
- le norme inerenti i sistemi informatici della Fondazione;
- in generale, la normativa applicabile.

In particolare, i soggetti coinvolti nelle aree di rischio sono tenuti al rispetto delle norme di comportamento di seguito indicate.
È fatto assoluto divieto:

- di porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 24-*bis* del D.lgs. n. 231/2001;
- di utilizzare postazioni informatiche diverse da quelle della Fondazione per lo svolgimento della propria attività lavorativa;
- di connettersi alla rete internet o di inviare messaggi di posta elettronica per motivi connessi alla propria attività di lavoro utilizzando un account diverso da quello fornito dall'Ufficio Sistemi informativi a ogni lavoratore (dipendente e/o collaboratore), in particolare, non si potranno utilizzare neppure da casa account personali;
- di utilizzare pc, portatili e pendrive diversi da quelli forniti dalla Fondazione laddove ci si trovi a lavorare in postazioni esterne alle sedi della Fondazione;
- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- di utilizzare la propria e altrui postazione informatica per scopi diversi da quelli conformi allo svolgimento delle mansioni attribuitegli;
- di trasmettere e ricevere posta elettronica per scopi diversi da quelli conformi allo svolgimento delle mansioni attribuitegli;
- di scaricare da Internet files e/o software non strettamente inerenti l'attività della Fondazione e senza espressa autorizzazione dei vertici della Fondazione;
- di installare programmi di alcun tipo non autorizzati dai vertici della Fondazione;
- di istallare, effettuare il downloading e/o utilizzare programmi e tools informatici che consentono l'introduzione abusiva all'interno di sistemi informatici o telematici protetti da

misure di sicurezza o che permettono la permanenza al loro interno, in violazione delle norme poste a presidio degli stessi dal titolare dei dati o dei programmi che si intende custodire o mantenere riservati;
- di reperire, diffondere, condividere e/o comunicare le modalità di impiego di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- di conoscere, registrare, trattare e divulgare i dati personali dei lavoratori (dipendenti e/o collaboratori), studenti o di terzi, se non espressamente autorizzati nelle forme e nei termini di cui al Regolamento UE n. 2016/679.

Pertanto, è obbligatorio il rispetto delle licenze, dei diritti d'autore e di tutte le leggi e i Regolamenti locali, nazionali ed internazionali che tutelano la proprietà intellettuale e le attività on-line.
È istituito un sistema di memorizzazione, utilizzando il Server aziendale, di tutti i dati di navigazione da tutte le postazioni informatiche della Fondazione, che potrà essere verificato, senza preavviso, dall'Organismo di Vigilanza, per un tempo retrospettivo di massimo 6 mesi.
Attraverso il server interno prescelto dalla Fondazione, potranno essere tracciati i flussi di navigazione e la posta elettronica in uscita da postazioni diverse da quelle della Fondazione, laddove vengano utilizzate le credenziali interne, sempre per un massimo di 6 mesi per quanto attiene alla navigazione e per 1 mese per la posta elettronica.
Lo stesso sistema di memorizzazione vige anche nelle ipotesi in cui l'utente, pur utilizzando un terminale esterno alla Fondazione, si colleghi ad un computer interno attraverso la rete internet (ad esempio, utilizzando software quali Teamviewer o similari come, ad esempio, connessione in VPN).
Vengono altresì memorizzati, per un tempo indefinito, tutti i contatti con i server interni da tutte le postazioni della Fondazione.
Dovrà essere istituito un sistema di controlli interno alla Fondazione che preveda la verifica del corretto utilizzo da parte dei dipendenti, dei collaboratori o dei responsabili incaricati delle password o dei codici di accesso ai sistemi informativi degli Uffici della P.A. (ad es.: PIN Agenzia delle Entrate o altri) e/o per l'utilizzo, in genere, delle postazioni informatiche.
Sarà fatto obbligo ai dipendenti e ai lavoratori autonomi (collaboratori) di modificare la password ogni tre mesi, ferma restando la dimensione minima di otto caratteri e la differenza rispetto alle ultime cinque password autocreate.
È fatto obbligo per ogni utente di bloccare la postazione ogni volta che questa viene abbandonata, anche semplicemente per recarsi ai servizi igienici. Le eventuali violazioni verranno segnalate all'Organismo di Vigilanza. Resta fermo che dopo 3 minuti di inutilizzo la postazione informatica si blocca automaticamente.
Dovranno essere istituiti indici rilevanti dell'attendibilità commerciale e professionale dei consulenti esterni in materia informatica; in particolare, gli stessi dovranno certificare la loro incensuratezza rispetto ai reati informatici.
È istituito un sistema di tracciabilità informatico dei rapporti intercorsi tra ogni lavoratore (dipendente e/o collaboratore) della Fondazione e gli incaricati dei Sistemi Informativi aventi ad oggetto ogni intervento riguardante la propria postazione informatica.
In caso di richieste verbali o telefoniche sarà istituito apposito registro degli interventi da parte dei responsabili dei sistemi informativi.

Dovrà essere svolta eventuale formazione dei lavoratori (dipendenti e/o collaboratori) concernente la normativa riguardante i reati informatici.
Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'ODV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.
L'ODV provvederà altresì al monitoraggio del sistema esistente e alle richieste di suo eventuale adeguamento in base alle caratteristiche specifiche della Fondazione da recepirsi a mezzo di revisione del presente Modello.

B.3. I FLUSSI INFORMATIVI

I soggetti interni coinvolti nelle aree a rischio di cui alla presente Parte Speciale B sono tenuti a comunicare all'ODV ogni violazione del presente Modello e/o del Codice Etico con tempestività.
In particolare, il Data Protection Officer (DPO) nominato ai sensi del Regolamento n. 2016/679 è il soggetto individuato dalla Fondazione per trasmettere all'ODV un report annuale contenente informazioni in merito a:

- danneggiamenti o guasti ai sistemi informatici non giustificabili in relazione ad un normale utilizzo dei medesimi;
- utilizzo improprio dei servizi internet e di posta elettronica;
- utilizzo improprio delle password per l'accesso alle postazioni informatiche e/o per l'accesso ai servizi di home banking e/o per l'accesso ai sistemi informatici di Enti Pubblici (MIUR; Agenzia delle Entrate, INPS, CCIAA, etc.);
- eventuali anomalie riscontrate nell'utilizzo di hardware e/o software di cui la Fondazione si è dotata;
- eventuali deroghe (motivate) alle procedure previste.

B.4. I COMPITI DELL'ORGANISMO DI VIGILANZA

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'ODV nello Statuto dell'ODV approvato dall'organo amministrativo della Fondazione, fermo restando il potere discrezionale dell'ODV di attivarsi con specifici controlli, periodicamente o a seguito delle segnalazioni ricevute in relazione alla prevenzione dei reati di cui alla presente parte speciale, l'ODV, tra l'altro, deve:

- verificare l'adeguatezza e l'aggiornamento della documentazione e delle procedure predisposte con riguardo alla prevenzione dei delitti informatici e al trattamento illecito dei dati;
- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati informatici;
- verificare il rispetto dei protocolli procedurali, con particolare riferimento alla gestione della sicurezza informatica;

- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- verificare variazioni ai profili di accesso alla rete e/o ai sistemi, alla funzionalità ed efficienza del sito internet;
- verificare, anche mediante controlli a campione ed ispezioni a sorpresa, la posta elettronica in entrata e in uscita e le connessioni ad internet nelle singole postazioni e anche sul server.

L'ODV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati informatici al Consiglio di amministrazione, secondo i termini indicati nel documento "*Reporting* dell'Organismo di Vigilanza".