Fondo Pensioni
per il personale cariplo

Parte speciale

E

Delitti informatici e trattamento illecito di dati

(art. 24 bis del D.Lgs. 231/2001)

OTTOBRE 2022

INDICE

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI
(art. 24 bis del Decreto)

[modificato dal D. Lgs. n. 7 e 8/2016 e dal D. Lgs. n. 105/2019]

1) Reati in tema di delitti informatici e trattamento illecito di dati

1.1 Le fattispecie di reato

La legge 28 marzo 2008, n. 48 in materia di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica" introduce alcune modifiche, tra l'altro, al Titolo VII (Dei delitti contro la fede pubblica), al Titolo XII (Dei delitti contro la persona), al Titolo XIII (Dei delitti contro il patrimonio) del Libro secondo del Codice Penale.
La legge in esame, inoltre, all'art. 7, prevede l'introduzione dell'articolo 24-bis nel novero dei reati presupposto di cui al Decreto legislativo 231/01, così ampliando la responsabilità amministrativa degli enti anche in relazione alla commissione di delitti informatici e trattamento illecito di dati.
Recita l'art. 7 "1. Dopo l'articolo 24 del Decreto Legislativo 8 giugno 2001, n. 231, è inserito il seguente "Art. 24- bis – (*Delitti informatici e trattamento illecito di dati*).
1 In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente Decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

Tale previsione legislativa estende la responsabilità amministrativa degli enti ai seguenti reati informatici:

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.): se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria

o programmi specificamente destinati ad elaborarli[1]. Pertanto i documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali.

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 uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o 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 a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio[2].

La suddetta fattispecie si realizza altresì nell'ipotesi in cui il soggetto agente, pur essendo legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema. Secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per il proseguimento di finalità differenti da quelle per le quali era stato autorizzato.

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 profitto 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 apparati, 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 uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-quater.

[1] Articolo aggiunto dall'art. 3, L. 23 dicembre 1993, n. 547.
[2] Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

La fattispecie si configura sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione , sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

Detenzione, diffusione e installazione abusiva 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, 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 sino a euro 10.329.

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 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 tre a otto anni se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato[3].

Questo reato si realizza quando qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o metta a disposizione di altri apparecchiature, dispositivi o programmi.

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

[3] Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.

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

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.): Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al 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[4].

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, e` 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 e` 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.
Tale reato si realizza, anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse 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 e` commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.): Se il fatto di cui all'articolo 635- quater e` 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 e` 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 e` reso, in tutto o in parte, inservibile, la pena e` 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 e` commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

[4] Articolo aggiunto dall'art. 9, L. 23 dicembre 1993, n. 547

Tale reato si realizza, anche nel caso in cui si tratti di sistemi informatici o telematici di proprietà di privati ma destinati al soddisfacimento di un interesse pubblico.

Frode informatica del certificatore 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 se 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, e` punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Tale reato è realizzabile solo da parte dei certificatori qualificati, o meglio, dei soggetti che prestano servizi di certificazione di firma elettronica qualificata.

Frode informatica aggravata dal fatto che venga commessa con sostituzione dell'identità digitale in danno di uno o più soggetti (art. 640 ter c.p. comma 3)

Il reato lo realizza chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico e telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri ingiusto profitto con altrui danno.

Il 14 agosto 2013 DL n. 93 è stata prevista un'aggravante aggiungendo *"se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti",*con lo scopo di rendere più efficace il contrasto del preoccupante fenomeno del cosiddetto "furto d'identità digitale". La pena prevista è la reclusione da due a sei anni e la multa da 600 a 3.000 euro.

Alcune definizioni:

- ***Credenziali:*** *insieme di elementi identificativi di un utente o di un account (generalmente User ID e Password),*
- ***Password****: sequenza di caratteri alfanumerici o speciali necessaria per autenticarsi ad un sistema informatico o ad un programma applicativo;*
- ***Postazione di lavoro****: postazione informatica aziendale fissa oppure mobile in grado di trattare informazioni;*
- ***Sicurezza Informatica****: insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici;*
- ***Virus****: programma creato a scopo di sabotaggio o vandalismo, in grado di alterare il funzionamento di risorse informatiche, di distruggere i dati memorizzati, nonché di propagarsi tramite supporti rimovibili o reti di comunicazione.*

Protocolli e indirizzi operativi di attuazione

1.2 Possibili ambiti di commissione del reato

Le attività del FPC nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.
Nell'ambito dello svolgimento delle normali attività aziendali potrebbero in ipotesi configurarsi i reati informatici innanzi indicati e, più in particolare, quelli inerenti l'alterazione di documenti aventi efficacia probatoria, la gestione degli accessi ai sistemi informativi interni o di concorrenti terzi e la diffusione di *virus* o programmi illeciti.

1.3 Principi di comportamento

I sotto indicati principi di comportamento, comuni a tutte le funzioni aziendali, dovranno essere applicati e rispettati dalle funzioni interessate.
I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione della strumentazione informatica del FPC devono attenersi alle modalità di utilizzo degli strumenti aziendali e, in generale, alle norme aziendali che danno attuazione ai seguenti principi:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi del FPC evitando che terzi soggetti possano venirne a conoscenza;
- aggiornare periodicamente le *password*, secondo le regole indicate dalla società;
- garantire la tracciabilità dei documenti prodotti attraverso l'archiviazione delle varie versioni dei documenti o comunque garantire meccanismi di tracciabilità delle modifiche;
- assicurare meccanismi di protezione dei *file*, quali *password*, conversione dei documenti in formato non modificabile.

E' fatto esplicito divieto di:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate dal FPC per finalità diverse da quelle lavorative;
- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- accedere, senza averne la autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure nel fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature,

dispositivi o programmi informatici 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, l'alterazione del suo funzionamento (il divieto include la trasmissione di *virus* con lo scopo di danneggiare i sistemi informativi di enti concorrenti).

- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento;
- distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ostacolarne gravemente il funzionamento;
- installare *software*/programmi aggiuntivi rispetto a quelli esistenti e/o autorizzati dalla funzione aziendale centrale dei Sistemi Informativi;
- introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione di Sistemi Informativi o altra funzione responsabile;
- modificare la configurazione di postazioni di lavoro fisse o mobili

Ai fini di una maggiore prevenzione delle fattispecie di reati in questione per la funzione interessata sono indicati di seguito i relativi principi organizzativi e di controllo, nonché le procedure, prassi, regolamenti aziendali a cui fare riferimento.

DIRETTORE SEGRETARIO

Principi organizzativi e di controllo

Ai fini della prevenzione le norme generali devono dare attuazione a quanto segue:

- devono essere definiti processi adeguati alle dimensioni ed ai profili di operatività del Fondo;
- le credenziali di accesso ai sistemi siano prontamente eliminate per il personale dimesso e ogni utente disponga di una *user* e *password* personale;
- bisogna assicurarsi che i terminali devono oscurarsi o scollegarsi dopo un periodo di inattività;
- l'utenza ed il profilo di accesso attribuito all'utente siano periodicamente rivisti per verificare se sussistono ancora le condizioni che hanno portato alla relativa attivazione;
- se necessario e/o tecnicamente possibile, le attività ritenute maggiormente critiche sono "registrate" in opportuni log, regolarmente ispezionati per garantire che gli utenti effettuino solo le attività per cui sono stati autorizzati.

- i *backup* dei dati residenti sui *server* siano salvati con frequenza giornaliera ed i supporti adeguatamente conservati;
- funzioni "privilegiate" devono essere concesse solo se ne esiste una reale necessità, sulla base di un'esigenza specifica e il loro utilizzo deve essere controllato;
- devono essere definiti dei controlli sulle applicazioni di sistema per verificare che non vi siano state delle modifiche non autorizzate.

Procedure, prassi, regolamenti interni, circolari, linee guida in essere
E' sufficiente quanto riportato nel Codice Etico e quanto indicato nel precedente punto principi di comportamento.
Si precisa che ha seguito della direttiva europea sulla privacy sono in fase di adeguamento alcune procedure informatiche per il trattamento dei dati.

PREVIDENZA SEZIONE II – SERVIZI ATTUARIALI E ASSICURATIVI
Principi organizzativi e di controllo
Ai fini della prevenzione le norme generali devono dare attuazione a quanto segue:

- devono essere definiti processi adeguati alle dimensioni ed ai profili di operatività del Fondo;
- le credenziali di accesso ai sistemi siano prontamente eliminate per il personale dimesso e ogni utente disponga di una *user* e *password* personale;
- bisogna assicurarsi che i terminali devono oscurarsi o scollegarsi dopo un periodo di inattività;
- l'utenza ed il profilo di accesso attribuito all'utente siano periodicamente rivisti per verificare se sussistono ancora le condizioni che hanno portato alla relativa attivazione;
- se necessario e/o tecnicamente possibile, le attività ritenute maggiormente critiche sono "registrate" in opportuni log, regolarmente ispezionati per garantire che gli utenti effettuino solo le attività per cui sono stati autorizzati.
- i *backup* dei dati residenti sui *server* siano salvati con frequenza giornaliera ed i supporti adeguatamente conservati;
- funzioni "privilegiate" devono essere concesse solo se ne esiste una reale necessità, sulla base di un'esigenza specifica e il loro utilizzo deve essere controllato;
- devono essere definiti dei controlli sulle applicazioni di sistema per verificare che non vi siano state delle modifiche non autorizzate.

Procedure, prassi, regolamenti interni, circolari, linee guida in essere
E' sufficiente quanto riportato nel Codice Etico e quanto indicato nel precedente punto principi di comportamento.
Si precisa che ha seguito della direttiva europea sulla privacy sono in fase di adeguamento alcune procedure informatiche per il trattamento dei dati.

CONTROLLO DI GESTIONE E AMMINISTRAZIONE SISTEMI INFORMATICI

I seguenti principi sono comunque da considerare anche se la funzione nell'ultima attività di valutazione dei rischi reato 231 (Risk assessment) non ha ritenuto questa famiglia di reato a potenziale rischio.

Principi organizzativi e di controllo

Ai fini della prevenzione le norme generali devono dare attuazione a quanto segue:

- devono essere definiti processi adeguati alle dimensioni ed ai profili di operatività del Fondo;
- le credenziali di accesso ai sistemi siano prontamente eliminate per il personale dimesso e ogni utente disponga di una *user* e *password* personale;
- bisogna assicurarsi che i terminali devono oscurarsi o scollegarsi dopo un periodo di inattività;
- l'utenza ed il profilo di accesso attribuito all'utente siano periodicamente rivisti per verificare se sussistono ancora le condizioni che hanno portato alla relativa attivazione;
- se necessario e/o tecnicamente possibile, le attività ritenute maggiormente critiche sono "registrate" in opportuni log, regolarmente ispezionati per garantire che gli utenti effettuino solo le attività per cui sono stati autorizzati.
- i *backup* dei dati residenti sui *server* siano salvati con frequenza giornaliera ed i supporti adeguatamente conservati;
- funzioni "privilegiate" devono essere concesse solo se ne esiste una reale necessità, sulla base di un'esigenza specifica e il loro utilizzo deve essere controllato;
- devono essere definiti dei controlli sulle applicazioni di sistema per verificare che non vi siano state delle modifiche non autorizzate.

Procedure, prassi, regolamenti interni, circolari, linee guida in essere

E' sufficiente quanto riportato nel Codice Etico e quanto indicato nel precedente punto principi di comportamento.

Si precisa che ha seguito della direttiva europea sulla privacy sono in fase di adeguamento alcune procedure informatiche per il trattamento dei dati

Flussi informativi verso l'Organismo di Vigilanza

Tutti i Destinatari coinvolti nella gestione dei sistemi informativi segnalano all'Organismo di Vigilanza qualsiasi eccezione comportamentale rispetto alle regole sopra indicate, nonché a quelle riportate nel Codice Etico e inoltre:

- eventuali tentativi di atti di "pirateria" accertati sui sistemi informativi;
- utilizzo di password non autorizzate, nonché scambi delle stesse tra soggetti diversi;
- intercettazione di modifiche non autorizzate da parte degli utenti;
- backup di dati non riusciti.

A completamento di quanto sopra è presente per singola Area/Funzione aziendale una scheda "Flussi informativi verso l'Organismo di Vigilanza" in cui sono indicate per fattispecie di reato, la specifica descrizione del flusso informativo da inviare all'OdV e la tempistica d'invio.