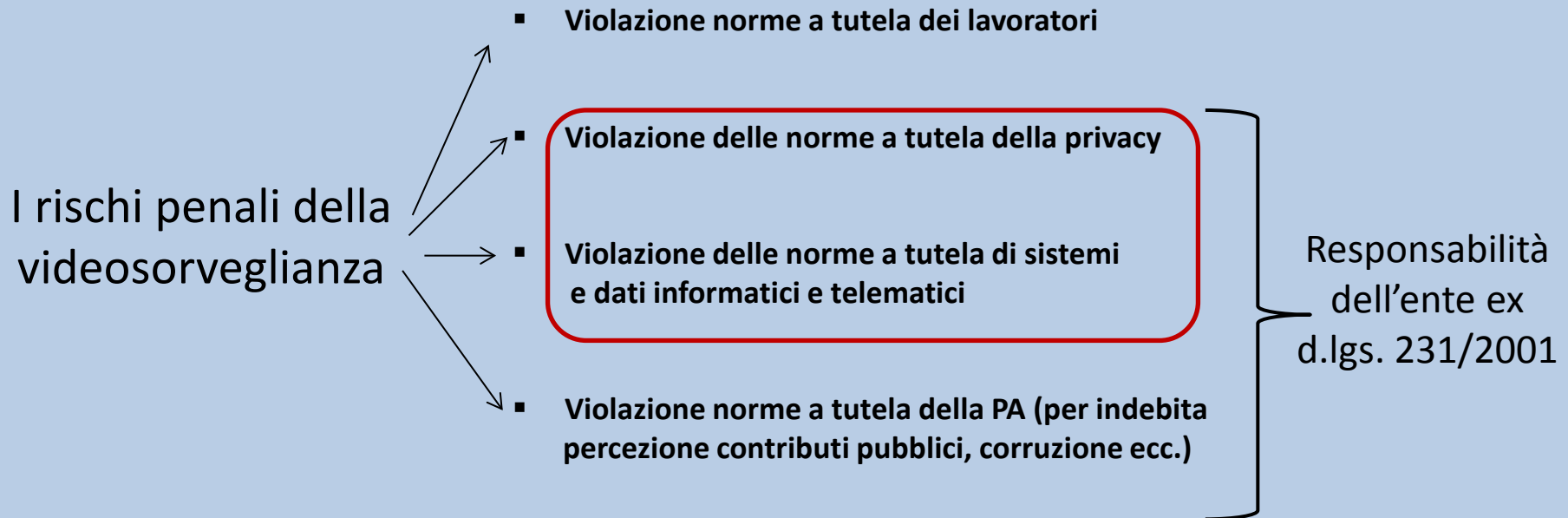


Osservatorio Settoriale sulle RSA

Delitti informatici e trattamento illecito di dati nel
sistema di compliance 231/2001

Avv. Marco Farina



I Parte: VIDEOSOERVEGLIANZA E TUTELA PENALE DELLA PRIVACY

ART. 167 (Trattamento illecito di dati) T.U. Privacy

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva documento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva documento, con la reclusione da uno a tre anni.

- ❑ *Fattispecie sussidiaria*
- ❑ *Procedibilità d'ufficio*
- ❑ *A forma vincolata (fattispecie sanzionatoria)*
- ❑ *Reato di evento*
- ❑ *Dolo generico e dolo specifico*

A proposito del delitto di *Trattamento illecito di dati*:

- È **trattamento** *“qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'inter-connessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati”*.
- È **dato personale** *“qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”*.
 - **dati identificativi**: quelli che *“permettono l'identificazione diretta dell'interessato”*;
 - **dati sensibili**: *“idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale”*;
 - **dati giudiziari**: quelli relativi al casellario giudiziale o alle pendenze penali.
- Il **nocumento** può avere ad oggetto effetti pregiudizievoli anche solo sotto il profilo morale dell'offeso, mentre il **profitto** può concretarsi in qualsiasi soddisfazione o godimento che l'agente si ripromette di ritrarre (Cass. 28280/2013)

ART. 615-bis c.p. (interferenze illecite nella vita privata)

Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso 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 servizio, o da chi esercita anche abusivamente la professione di investigatore privato

- ❑ *Delitto più grave del 167*
- ❑ *Procedibilità a querela salvo eccezioni*
- ❑ *Reato di mera condotta*
- ❑ *Dolo generico*
- ❑ *Fattispecie ad illiceità espressa*

A proposito del delitto di *interferenze illecite*:

- Il rinvio all'art. 614 c.p. richiama la nozione di **domicilio**, inteso come «abitazione o altro luogo di privata dimora o sue pertinenze»:



- L'avverbio **abusivamente** sottolinea la necessità di verificare se la condotta fosse in qualche modo giustificata alla luce di esigenze riconosciute e tutelate dall'ordinamento: rinvio alla normativa di settore.

La *ratio* ispiratrice della legge regionale n. 2/2017 (contrasto e prevenzione dei casi di maltrattamento) - che avrebbe potuto orientare nella individuazione dei limiti di liceità della videosorveglianza - non trova chiaro riflesso nel testo normativo:

≠

Art. 3 del progetto di legge: le registrazioni sono effettuate in modalità criptata nel rispetto di quanto previsto dal d.lgs. 196/2003 e delle altre normative vigenti in materia e possono essere visionate secondo quanto previsto dal codice di procedura penale.

Art. 3 del testo promulgato: le registrazioni sono effettuate nel rispetto di quanto previsto dal d.lgs. 196/2003, dalle altre normative vigenti in materia e dalle prescrizioni impartite dal Garante per la protezione dei dati personali

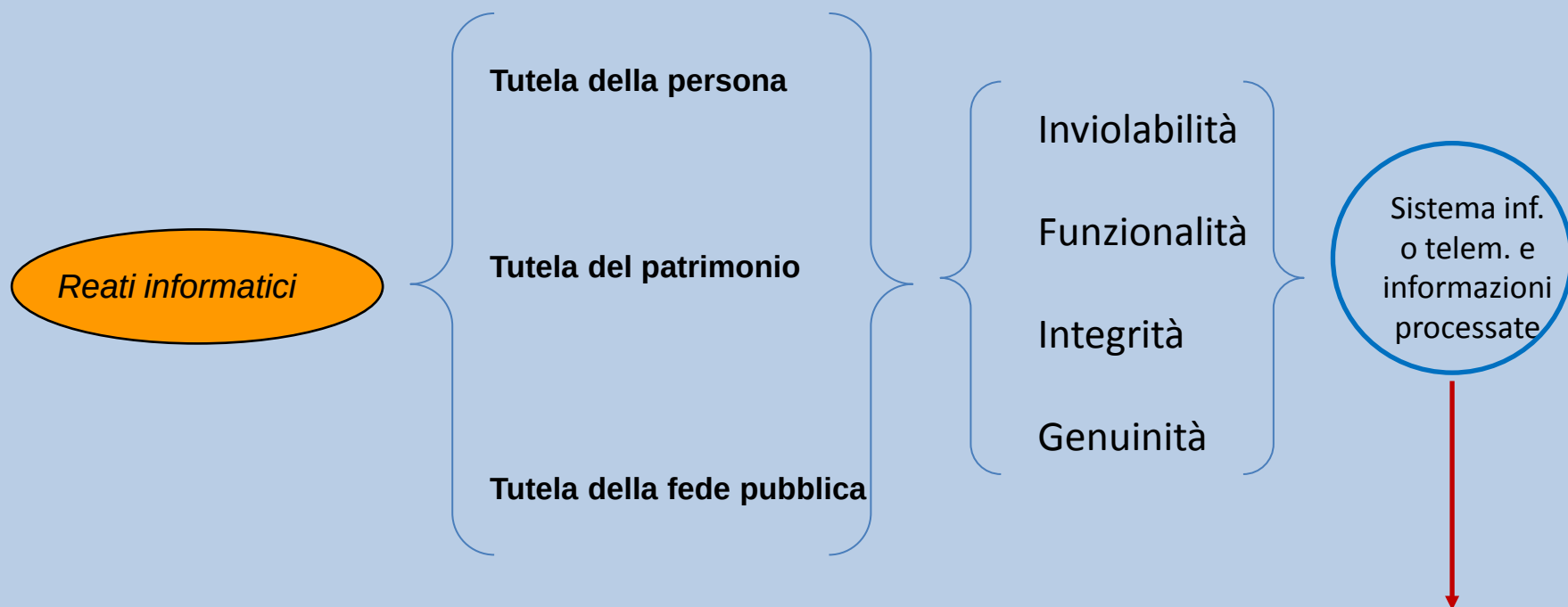
Sarà la giurisprudenza a chiarire funzioni e limiti di utilizzabilità della videosorveglianza di cui alla LR 2/2017:

Registrazioni che violano privacy
Costituiscono reato (167)
Utilizzabili per provare i fatti documentati

Registrazioni che violano il domicilio
Costituiscono grave reato (615-bis)
Inutilizzabili per provare i fatti documentati

Registrazioni che rispettano privacy
Sono lecite
Utilizzabili per provare i fatti documentati

II Parte: VIDEOSOERVEGLIANZA E TUTELA PENALE DEI SISTEMI E DEI DATI INFORMATICI E TELEMATICI



- *«Per sistema informatico deve intendersi qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali, secondo un programma svolga un trattamento automatico di dati, sicché vi rientra un sistema di videosorveglianza che, composto da alcune videocamere che registrano le immagini e le trasformano in dati, si avvalga anche di un hard disk che riceve e memorizza immagini, rendendole estraibili e riproducibili per fotogrammi» (Cass. n. 9870/2011)*

a) Fattispecie a tutela dell'inviolabilità del sistema

615-ter Accesso abusivo ad un sistema informatico o telematico

Chiunque **abusivamente** si introduce in un **sistema informatico o telematico** protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

615-quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, **abusivamente** si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un **sistema informatico o telematico**, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro.

615-quinquies Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare **illecitamente** un **sistema informatico o telematico**, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

a) Fattispecie a tutela dell'inviolabilità del sistema

- Che cosa deve intendersi per “accesso” abusivo?

È abusivo – a prescindere dalla sue finalità – anche il mero accesso ‘logico’ ad un sistema informatico o telematico effettuato mediante la violazione delle misure di protezione poste a tutela dello stesso, da parte di soggetti non abilitati ad interfacciarsi con il sistema medesimo.

- In che cosa consistono le “misure di protezione”?

Ai fini della normativa penale, sono “misure di protezione” gli accorgimenti adottati per limitare l'accesso ad un sistema informatico o telematico, ivi inclusi non solo i presidi logici – password o filtri telematici – ma anche le barriere fisiche fraposte tra l'utente e la macchina.

B) Fattispecie a tutela della funzionalità del sistema

617-quater

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Chiunque **fraudolentemente intercetta** comunicazioni relative ad **un sistema informatico o telematico** o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da 6 mesi a 4 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.

617-quinquies

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche

Chiunque, **fuori dai casi consentiti dalla legge**, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad **un sistema informatico o telematico** ovvero intercorrenti tra più sistemi, è punito con la reclusione da 1 a 4 anni.

617-sexies

Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

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 ad 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 1 a 4 anni.

c) Fattispecie a tutela dell'integrità del sistema (e dei dati)

635-bis

**Danneggiamento di informazioni,
dati e programmi informatici**

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da 6 mesi a 3 anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da 1 a 4 anni

635-ter

**Danneggiamento di informazioni,
dati e progr. informatici utilizzati
dallo Stato o da altro ente pub. o
comunque di pub. utilità**

Punito il tentativo + aggravante per ipotesi consumata o uso di violenza/abuso qualità di operatore del sistema

635-quater

**Danneggiamento di sistemi
informatici o telematici**

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 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 1 a 5 anni.
Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

635-quinquies

**Danneggiamento di sistemi infor.
o telem. di pub. utilità**

Punito il tentativo + aggravante per ipotesi consumata o uso di violenza/abuso qualità di operatore del sistema

d) Fattispecie a tutela della genuinità del sistema e dei dati processati

640-ter

Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

640-quinquies

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

491-bis

Documenti informatici

Se alcuna 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

III Parte: VIDEOSOERVEGLIANZA E RESPONSABILITÀ DA REATO DELL'IMPRESA

Tradizionalmente: *societas delinquere non potest*

Gli enti e le persone giuridiche possono rispondere per fatti di reato, solo in via mediata e indiretta (responsabile civile, civilmente obbligato)

In anni recenti:

- Riflessione criminologica sui c.d. White Collar Crimes
- Esperienza comparatistica;
- Convenzioni internazionali

Il d.lgs. 8 giugno 2001, n. 231: “**responsabilità amministrativa da reato**”

Le ipotesi originarie:

- Concussione e corruzione (art. 25);
- Indebita percezione di erogazioni, truffa e frode inform. contro lo Stato (art. 24);

Le ipotesi successive:

- **Progressiva estensione dei «reati presupposto»:**
«Per il delitto di cui all'art. X c.p., si applica all'ente la sanzione di N quote»

L. 18 marzo 2008, n. 48



Art. 24-bis D.lgs. 231/2001

Delitti informatici e trattamento illecito di dati

Art. 24-bis D.lgs. 231/2001

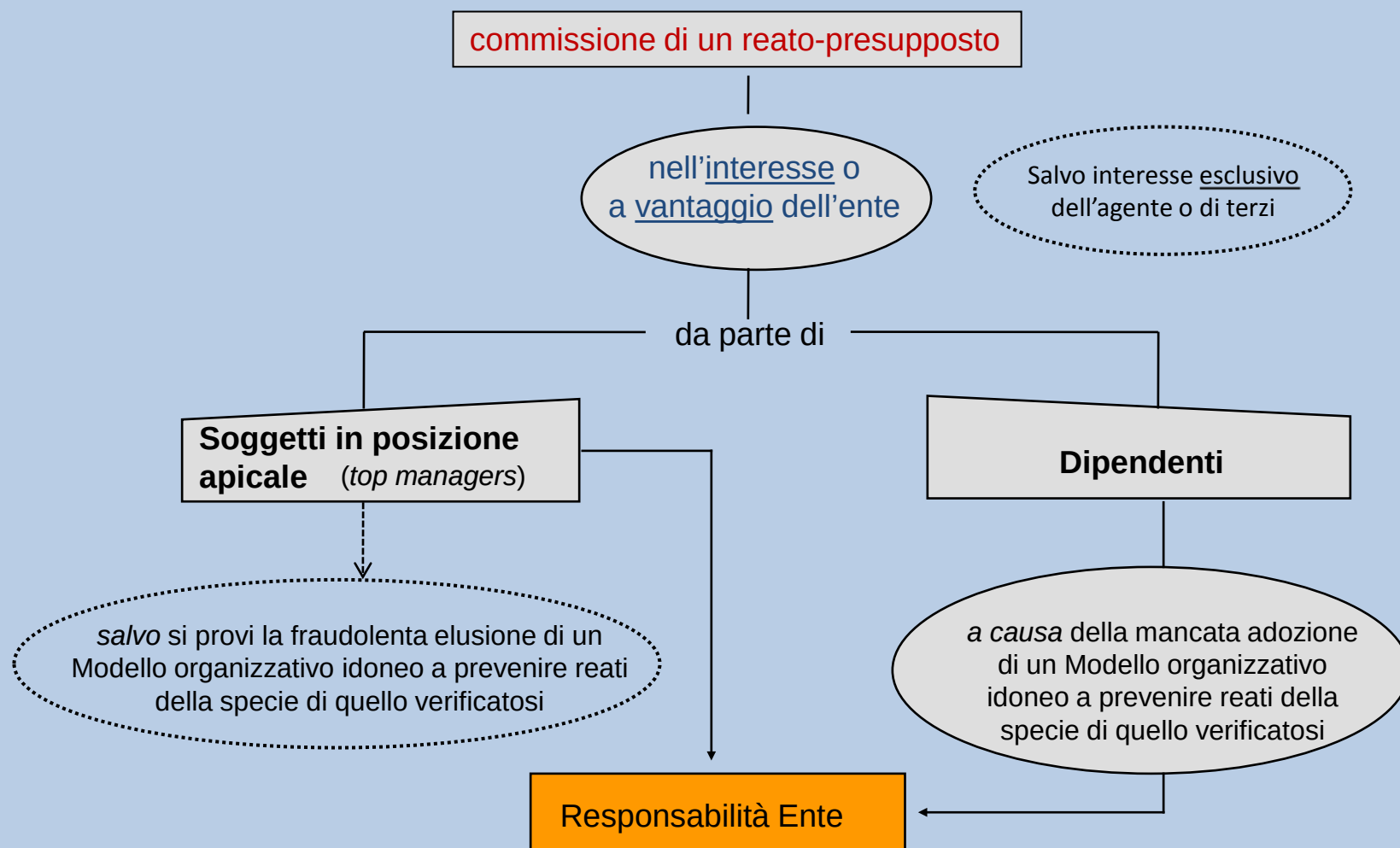
Delitti informatici e trattamento illecito di dati

Delitti informatici		Sanzioni per l'ente
 615-ter c.p.: accesso abusivo ad un sistema informatico o telematico	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
 617-quater c.p.: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
 617-quinquies c.p.: installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
▪ 635-bis c.p.: danneggiamento di informazioni, dati e programmi informatici	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
▪ 635-ter c.p.: danneggiamento di inform., dati e progr. inf. utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
▪ 635-quater c.p.: danneggiamento di sistemi informatici o telematici	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
▪ 635-quinquies c.p.: danneggiamento di sistemi informatici o telematici di pubblica utilità	→	▪ 100 ≤ quote ≥ 500 + sanzione interdittiva
▪ 615-quater c.p.: detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	→	▪ quote ≥ 300 + sanzione interdittiva
▪ 615-quinquies c.p.: diffusione di apparecchiature, dispositivi o progr. informatici diretti a danneggiare o interrompere un sistema inf. o telem.	→	▪ quote ≥ 300 + sanzione interdittiva
▪ 491-bis: (falso in) documenti informatici	→	▪ quote ≥ 400 + sanzione interdittiva
▪ 640-quinquies c.p.: frode informatica del soggetto che presta servizi di certificazione di firma elettronica	→	▪ quote ≥ 400 + sanzione interdittiva

Reati contro la privacy

167 d.lgs. 196/2003: trattamento illecito di dati →
[615-bis c.p.: interferenze illecite nella vita privata]





N.B.: In giurisprudenza si è affermato che l'interesse e/o il vantaggio dell'ente possono consistere anche nel risparmio di spesa derivante dall'omessa adozione di adeguati presidi volti ad evitare la commissione di illeciti. Il principio – affermato in relazione a reati presupposto colposi – si presta a pericolose interpretazioni estensive (vantaggio = risparmio derivante dall'omessa adozione del Modello) anche in relazione a tutti gli altri reati presupposto

Responsabilità dell'ente per reati informatici connessi all'attività di videosorveglianza

Nozione rigorosa di
interesse/vantaggio

Ente responsabile se è ravvisabile un interesse/vantaggio insito nel tipo d'illecito.

Casistica: accesso abusivo, danneggiamento dati o intercettazione del flusso delle immagini, per occultare situazioni pregiudizievoli all'azienda (come ad esempio episodi di maltrattamento o malasanità) o per acquisire informazioni da utilizzare impropriamente a beneficio dell'ente (ad esempio per costringere un dipendente alle dimissioni volontarie)

Nozione estensiva di
interesse/vantaggio
(= risparmio di spesa)

Ente responsabile quando l'illecito sia dovuto alle inadeguate risorse investite nei presidi per la sicurezza informatica o telematica o per l'implementazione del Modello organizzativo

Casistica: accesso abusivo, intercettazione del flusso di immagini o detenzione abusiva dei codici di accesso effettuati dai dipendenti/dirigenti anche solo per semplificare o sveltire l'attività lavorativa

Il contenimento dei rischi da reato

