GRANDE STEVENS

STUDIO LEGALE ASSOCIATO

AIGI

ASSOCIAZIONE ITALIANA
GIURISTI DI IMPRESA

"*Internal investigations,* controlli difensivi e tutela del patrimonio aziendale"

6 novembre 2023 - ore 17.00

NH Hotel Centro

TORINO

Avv. Nicola Menardo — Avv. Diego Saluzzo

INDICE

A) Le investigazioni interne: dai principi generali alle applicazioni pratiche

- principi generali, direttrici ed eterogeneità dei fini
- verifiche ordinarie / controlli difensivi su strumenti informatici
- accertamento di condotte di sottrazione di dati e documenti aziendali da parte dei dipendenti
- ruolo delle internal investigations nella disciplina del whistleblowing (D.LGS. N. 24/2023)

B) Dalla patologia alla prevenzione: modalità e best practices per la tutela del patrimonio aziendale

- evoluzione del concetto di patrimonio aziendale: gli «immaterials»
- tutela della proprietà intellettuale
- tutela di software e banche dati
- compliance integrata e corporate governance
- ESG e sostenibilità aziendale

GRANDE STEVENS
STUDIO LEGALE

A

Investigazioni interne: dai principi generali alle applicazioni pratiche

GRANDE STEVENS
STUDIO LEGALE

“Niente ha il potere di allargare tanto la mente quanto l’investigazione sistematica dei fatti che si possono osservare”
(Marco Aurelio)

Le investigazioni interne

- Processo di progressiva responsabilizzazione delle imprese - *self regulation* e *risk management*

- Investigazioni interne = strumento di *compliance* (polifunzionali)
  - ➞ verifica rispetto policy, procedure e codici aziendali
  - ➞ accertamento fatti illeciti:
    - ⊙ in danno dell'impresa
    - ⊙ che possono comportare responsabilità impresa (231)

- *"Diritto di difendersi provando"*
- collaborazione processuale *(self reporting USA)*

Le investigazioni interne

- MANCA UNA DISCIPLINA AD HOC

- Referente normativo più prossimo: indagini difensive (art. 391 bis e ss. c.p.p.) - LEGAL PRIVILEGE
  - ➞ prove dichiarative
  - ➞ prove documentali
  - ➞ ricognizioni (ispezioni, rilievi, sopralluoghi, CT)
  - ➞ prove atipiche ex art. 189 c.p.p.

Le fasi dell'*internal investigation*

1. RICEZIONE DELLA NOTIZIA
   - fonti interne (odv, internal audit, whistleblowing, data analysis report)
   - fonti esterne (reclami, stampa, ispezioni, indagini penali)
2. DATA COLLECTION PLAN
   - studiare il contesto di riferimento
   - determinare l'obiettivo dell'indagine e pianificare modalità esecutive (evitare overflow informativi)
3. FASE ESECUTIVA
   - acquisizione dati, documenti e dichiarazioni (interviste)
   - Rispetto dei limiti derivanti da ordinamento (privacy, Statuto dei Lavoratori, price sensitivity)
4. REPORT DI AUDIT
   - Relazione scritta all'ODV: natura descrittiva e dati obiettivi, nessuna valutazione/ipotesi
   - *Remediation plan* se rilievi di non conformità delle procedure vigenti
   - *Follow up* di audit

Le internal investigations e l'eterogenesi dei fini

- LEGAL PRIVILEGE circoscritto alle attività svolte dagli avvocati iscritti all'albo (artt. 103, 200, 256 c.p.p.)

- Potenziali effetti indesiderati delle *internal investigations*:
  - ➞ verbali, relazioni, report, corrispondenza sono assoggettabili a sequestro probatorio
  - ➞ internal auditors, componenti ODV, legal counsel e ogni altro soggetto appartenente all'organizzazione dell'impresa può essere sentito a s.i.t. con obbligo di verità
  - ➞ gli stessi soggetti possono essere esaminati in qualità di testimoni nel corso del giudizio - no segreto professionale
  - ➞ documenti acquisti e sequestrati saranno pienamente utilizzabili in giudizio quali prove documentali

Le internal investigations e l'eterogenesi dei fini

- POSSIBILE SOLUZIONE: indagini difensive ex art. 391 bis c.p.p. da parte di professionista esterno, in base allo scenario:

  (A) notizia di violazione che non integra illecito penale: investigazioni interne

  (B) notizia di violazione che integra illecito penale:

  ➞ reato in danno dell'ente - indagini miste (indagini difensive preventive)

  ➞ reato da responsabilità 231 - indagini difensive

- VANTAGGI:

  ✓ Legal privilege

  ✓ Svolgimento delle indagini con le forme e modalità ex art. 391 bis e ss. c.p.p. garantisce più elevato standard utilizzabilità prove favorevoli in giudizio

  ✓ No obbligo ostensione prove acquisite che si dimostrano sfavorevoli

  ✓ Documenti e atti d'indagine difensiva non possono essere acquisite al procedimento se non per iniziativa e su impulso del difensore

VERIFICHE ORDINARIE E CONTROLLI DIFENSIVI A TUTELA DEL PATRIMONIO AZIENDALE

Verifiche sugli strumenti informatici aziendali

- VERIFICA attività dei dipendenti è una delle declinazioni più critiche della tutela del patrimonio aziendale

- Fattori che rendono imprescindibile tale monitoraggio:
  - ➞ accresciuta mobilità dei lavoratori tra aziende
  - ➞ gestione dati aziendali tramite strumenti informatici
  - ➞ lavoro agile e circolazione *extra moenia* dei dati digitali

- DUE TIPOLOGIE DI CONTROLLI:
  - ✓ Controlli c.d. Ordinari - sull'attività day by day, per esigenze di protezione del sistema informatico e tutela preventiva del patrimonio aziendale
  - ✓ Controlli c.d. Difensivi - di carattere eccezionale, a fronte dell'emersione di circostante indicative della commissione di illeciti in danno dell'impresa

Verifiche sugli strumenti informatici aziendali

- CONTROLLI ORDINARI - DUE CATEGORIE DI LIMITI
  - ✓ STATUTO DEI LAVORATORI (art. 4)
    - Post Job Act 2015 legittime le verifiche sugli applicativi informatici in dotazione al lavoratore per svolgimento menzione e su strumenti rilevazione accessi e presenze
      - ➞ no preventivo accordo
      - ➞ dovere di informativa al lavoratore - *policy* formalizzate
  - ✓ G.D.P.R.
      - ➞ principi liceità, correttezza e trasparenza - *accountability*
      - ➞ finalità trattamento predeterminate e limitate

Verifiche sugli strumenti informatici aziendali

- CONTROLLI DIFENSIVI (post Jobs Act 2015)
  - ✓ No tutela preventiva ed ex ante del patrimonio aziendale
  - ✓Accertamento ex post della commissione di un illecito da parte del lavoratore, in danno dell'impresa o di terzi e finalità di difesa interessi dell'ente in giudizio

- I controlli difensivi sono diversi e ulteriori da quelli previsti dall'art. 4 Statuto Lavoratori e non sono assoggettati a tale disciplina

- Condizioni di liceità delineate dalla giurisprudenza (Ita e CEDU, Lopez Ribalda c. Spagna)
  - ➞ informazione del lavoratore sulle verifiche eseguibili
  - ➞ sussistenza di concreti ed effettivi elementi di sospetto a carico del lavoratore
  - ➞ verifiche circoscritte dal punto di vista soggettivo, oggettivo e temporale
  - ➞ rispetto principi di necessità, proporzionalità e minimizzazione dell'ingerenza

L’ACCERTAMENTO DI CONDOTTE DI SOTTRAZIONE DI DATI E DOCUMENTI AZIENDALI DA PARTE DEI DIPENDENTI

La sottrazione di dati informatici

- REATI configurabili a carico del dipendente infedele:
  - ✓ Art. 615 ter c.p.: accesso abusivo a sistema informatico
    - ➞ introduzione (accesso *invito domino*)
    - ➞ mantenimento (introduzione lecita, attività illecita)
  - ✓ Art. 646 c.p.: appropriazione indebita aggravata
    - ➞ documenti cartacei
    - ➞ dati aziendali copiati e poi cancellati dal server
- Due differenti prospettive di rischio
  a. il dipendente sottrae dati alla società - investigazioni interne con tutele viste
  b. l'impresa assume nuovo dipendente che utilizza dati sottratti (art. 648 c.p. ricettazione)
    - ➞ ex ante: valutazione rischio importazione illecita di dati e adozione procedure
    - ➞ ex post: indagini difensive ex art. 391 bis c.p.p. per evitare sanzioni 231

IL RUOLO DELLE INTERNAL INVESTIGATIONS NELLA DISCIPLINA DEL WHISTLEBLOWING (D.LGS. N. 24/2023)

La nuova disciplina del whistleblowing

- D.LGS. 24/2023 recepisce e attua Direttiva UE 2019/1937 e abroga disciplina precedente
- Non si applica più solo al settore pubblico e ai c.d. “reati 231” ma ad una categoria assai più ampia di illeciti di vario genere
- I segnalanti possono avvalersi di peculiari procedure di segnalazione (canali interni, esterni, divulgazione pubblica) e beneficiare del regime di protezione, che variano in base alla natura pubblica o privata dell’ente e all’ oggetto della segnalazione
- Ulteriori criteri applicativi del settore privato: dimensioni dell’ente, settore di operatività, presenza di Modello 231
- Forte ruolo ANAC anche nel settore privato: gestione dei canali di segnalazione esterna e tutela del segnalante con potere sanzionatorio amministrativo
- Espressa previsione di obblighi di istruttoria da parte dell’ente che riceve la segnalazione

La rilevanza delle internal investigations

1. Adempimento alle disposizioni del D.Lgs. n. 24/2023
   - "Gestione della Segnalazione"
     - ✓ settore pubblico: Responsabile Protezione Corruzione e Trasparenza (RPCT)
     - ✓ settore privato: no individuato *ex lege*, può essere organo di internal audit, ODV231 (linee guida Confindustria), esterno
   - "*Svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti*" (circolare ANAC) - anche audizione del segnalato

2. Qualora venga accertata l'insussistenza o la manifesta infondatezza dei fatti oggetto di segnalazione, la stessa deve essere archiviata.
   - Fase eventuale: non pare precluso all'ente adottare iniziative di investigazione interna per verificare se il fatto rientra comunque nei casi di protezione o se il segnalante può essere perseguito per la segnalazione effettuata:
     - ➞ per insussistenza dei presupposti di fondato motivo ex ante della segnalazione, sia sulla veridicità dell'informazione che sulla sua rilevanza ex d.lgs. 24/2023 (nb: esenzione anche per diffusione dati coperti da segreto, stesso presupposto)
     - ➞ per segnalazioni effettuate con modalità non conformi a quelle previste dal d.lgs. 24/2023
     - ➞ per l'iniziativa del segnalato che presenti denuncia querela per calunnia e/o diffamazione o agisca giudizialmente in sede civile fornendo elementi a sostegno del dolo/colpa grave del segnalante

B

Dalla patologia alla prevenzione: modalità e prassi per la miglior tutela del patrimonio aziendale

GRANDE STEVENS
STUDIO LEGALE

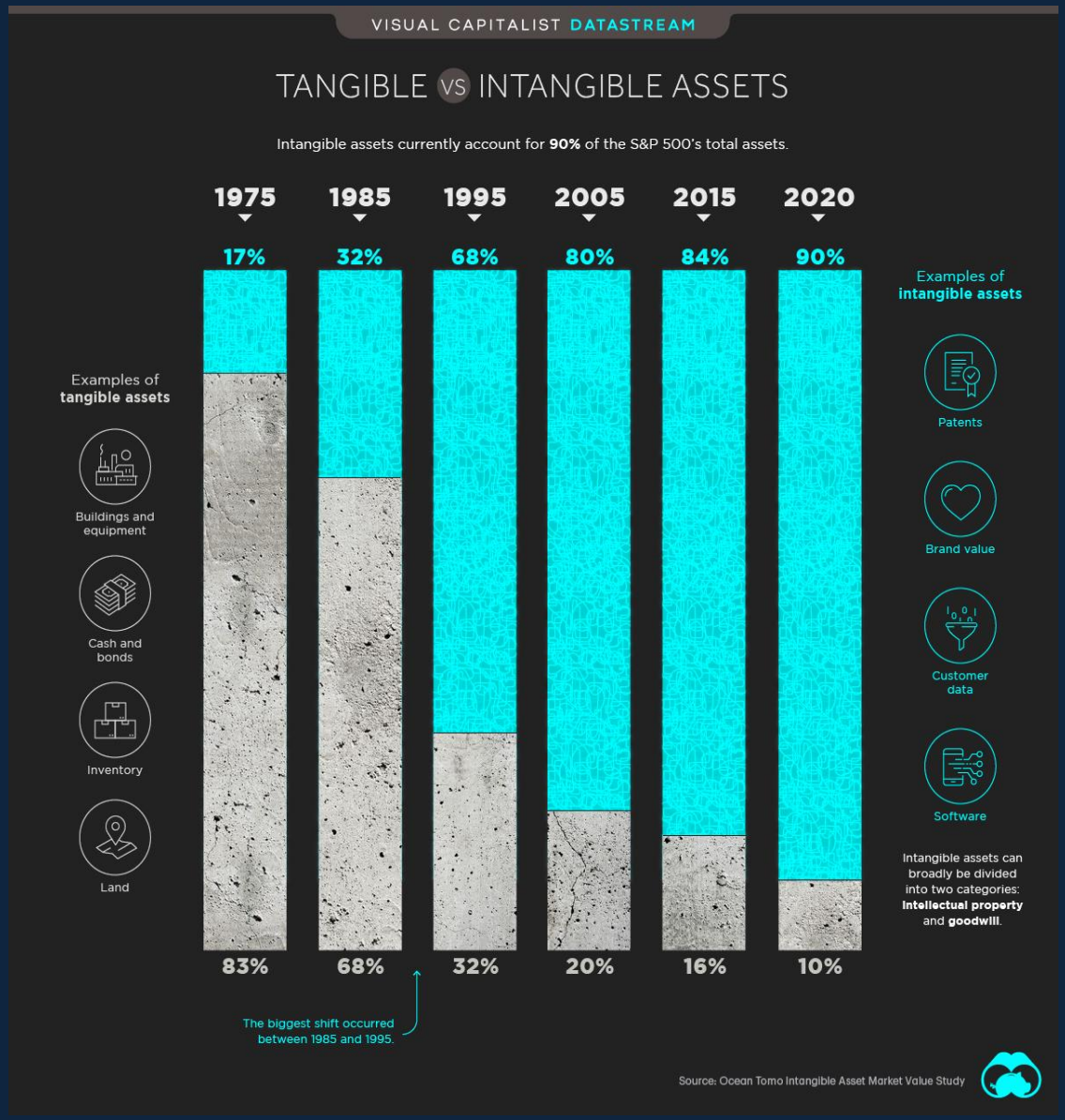
Evoluzione del concetto di patrimonio aziendale: gli «immaterials»

Patrimonio aziendale immateriale o intangibile = patrimonio di conoscenze dell'azienda e capacità in grado di creare valore e renderla competitiva, ma non facilmente traducibile in termini economico-finanziari

Evoluzione del concetto di patrimonio aziendale: gli «immaterials»

Proprietà intellettuale = diritto d'autore, brevetti, marchi, know how, segreti commerciali)
Capitale relazionale = immagine dell'azienda percepita dal mercato / valore reputazionale
Capitale umano = insieme di relazioni legate alla personalità di chi lavora in azienda
Corporate Governance = insieme di procedure e regole che permettono all'azienda di funzionare

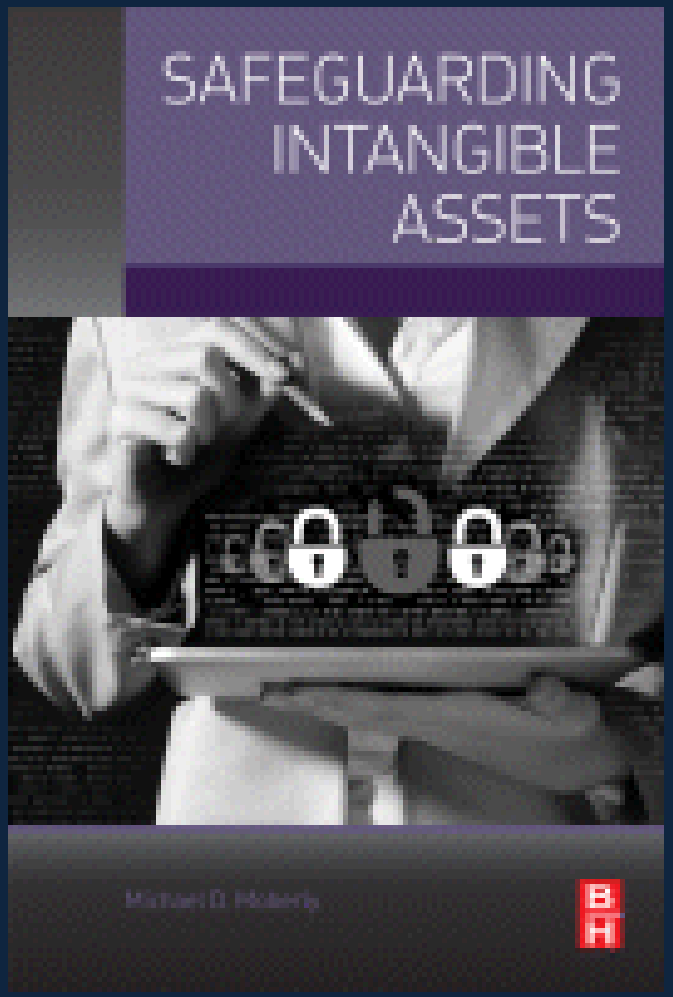
Evoluzione del concetto di patrimonio aziendale: gli «immaterials»



- Il patrimonio immateriale rappresenta oggi tra l'80% e il 90% del valore dell'intera azienda e vanno pertanto adeguatamente protetti da comportamenti scorretti e sleali, interni ed esterni

- Proteggere i propri asset immateriali è fondamentale per la competitività di un'azienda nel mercato: le aziende che raggiungono i risultati migliori in termini di successo, sono quelle che sfruttano al meglio le proprie risorse intangibili

Tutela del patrimonio aziendale immateriale



L’iniziativa volta a salvaguardare in prevenzione il patrimonio immateriale dell’azienda deve articolarsi su più fronti, perché il concetto di proprietà intellettuale è dinamico e la capacità di generare valore competitivo impone una corretta gestione e un efficace sfruttamento di tale patrimonio cognitivo sul mercato

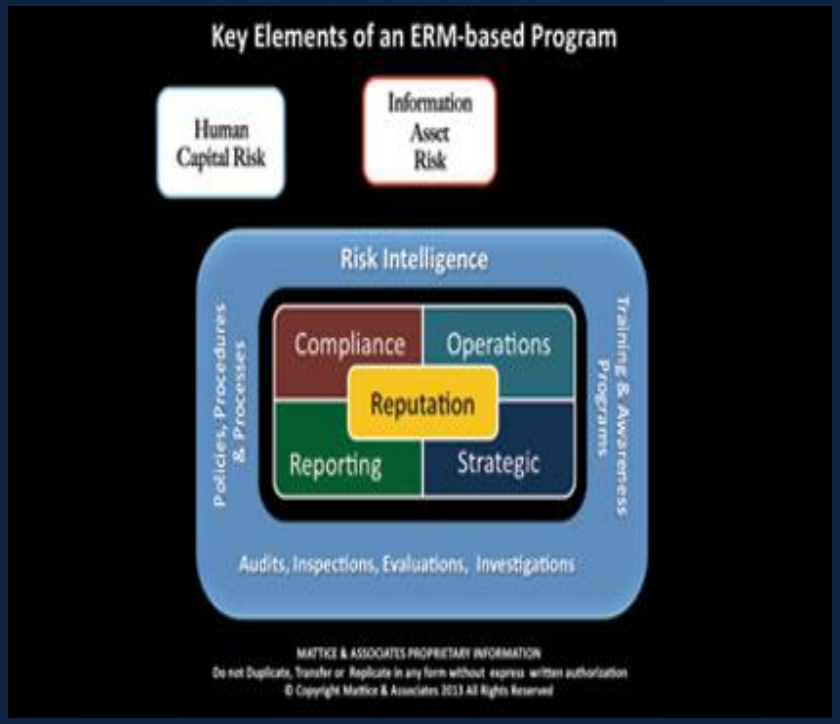
Gli strumenti di tutela sono però ancora troppo connotati da strumenti di difesa fisica, abbinati a strumenti di natura inibitoria e/o coercitiva, come i sistemi antintrusione, le procedure e le check list da osservare da parte dei dipendenti

Questo non è sufficiente ed occorre passare ad un approccio proattivo e olistico, guardando non solo al rispetto degli obblighi imposti dalle norme, ma alle opportunità che una compliance integrata può offrire

Tutela del patrimonio aziendale immateriale

La strutturazione di un sistema di tutela del patrimonio immateriale rappresenta pertanto per gli in-house counsel non tanto un rischio legato al non aver predisposto difese adeguate, quanto un’opportunità per acquisire un ruolo strategico in azienda, salvaguardando vantaggi competitivi e, in alcuni casi, facendosi profit center

Tutela del patrimonio aziendale immateriale

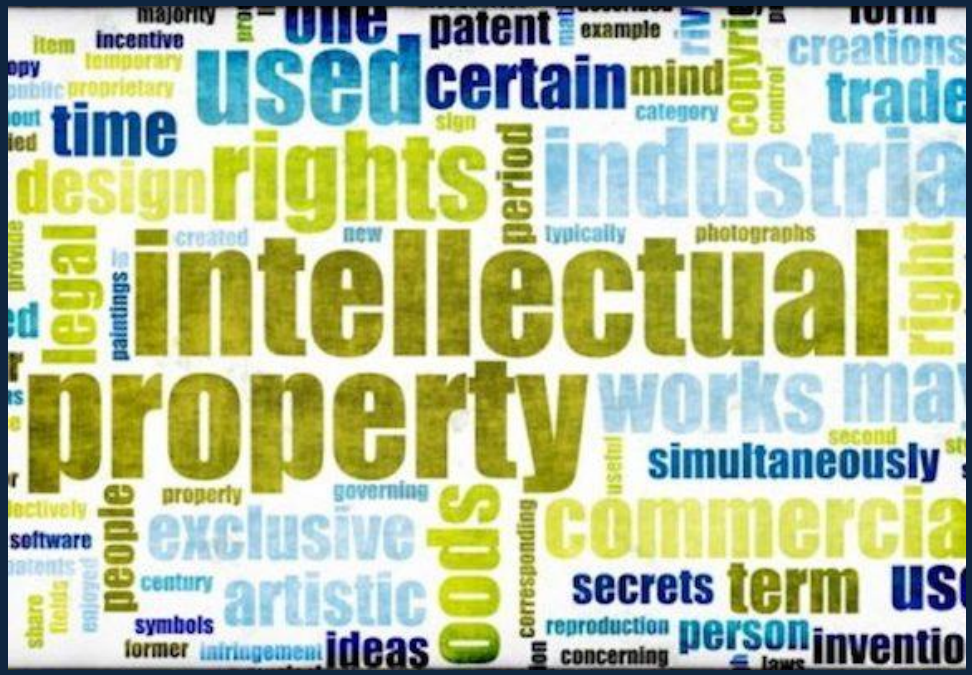


Nell'Enterprise Risk Management (ERM), nell'ambito del Sistema di Controllo Interno (SCI), rientra l'insieme delle regole, dei controlli e di ogni altra forza che contribuisce a mantenere l'organizzazione aziendale costantemente orientata al perseguimento dei seguenti obiettivi:

- salvaguardia del patrimonio aziendale
- efficacia ed efficienza delle operazioni
- conformità delle operazioni a leggi e regolamenti;
- affidabilità e integrità delle informazioni (ivi comprese le informazioni finanziarie e di bilancio)

Tutela della proprietà intellettuale

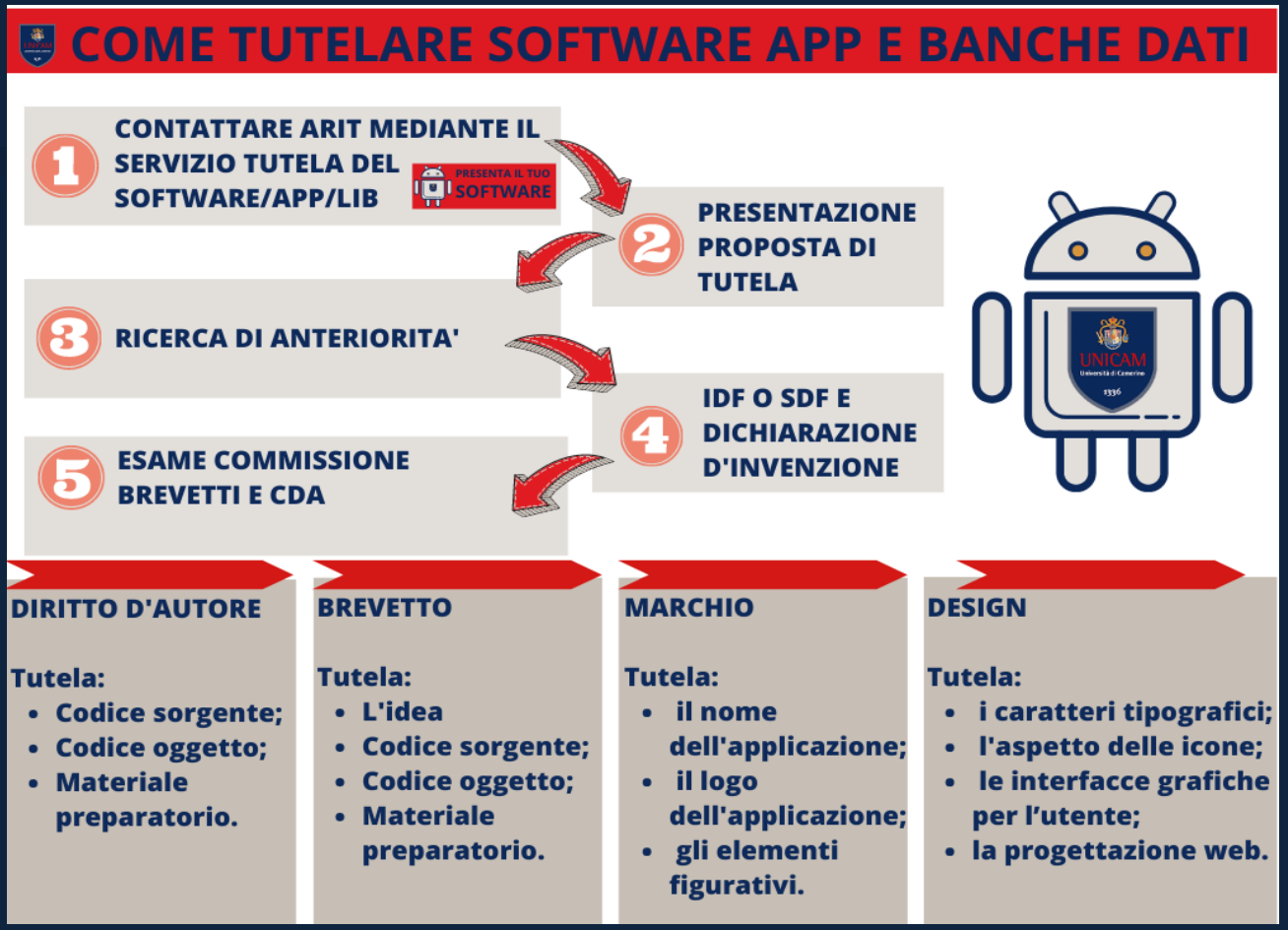
- conoscenza del proprio patrimonio immateriale
- adozione di adeguate strategie di protezione
- proprietà industriale: marchi brevetti e segni distintivi
- diritto d'autore / copyright: tutela del software, prodotti IT, di banche dati, di opere artistiche o letterarie, comprensive della pubblicità
- accordi di riservatezza
- clausole contrattuali



Tutela del software

- Unica tutela prevista espressamente dalla legge è quella relativa al diritto d'autore, ai fini di non limitare il principio di concorrenza
- Copyright Approach vs Patent Approach brevettabilità limitata sole se parte di sistema complesso
- Legge 22 aprile 1941, n. 633, concernente protezione del diritto d'autore e di altri diritti connessi al suo esercizio.
- Legge 20 giugno 1973, n. 399 di ratifica ed esecuzione della Convenzione di Berna per la protezione delle opere letterarie ed artistiche
- Anche a livello internazionale con l'accordo TRIPs il software, nei suoi codici sorgente e codici oggetto, viene equiparato alle opere letterarie

Tutela del software e banche dati



Tutela delle banche dati

- D.L. 6 maggio 1999, n. 169: Attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati

- Direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione

- Banca Dati = raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo tutelata se e in quanto " …per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore"

- La tutela è accordata ai criteri che sono alla base del suo funzionamento: ad es. modalità di accesso e di ricerca, che devono essere più di uno

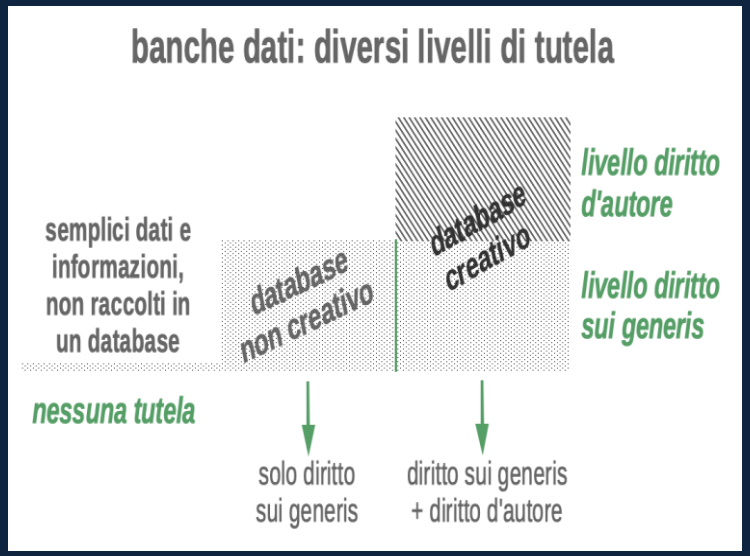
- La tutela delle banche dati in base al diritto di autore non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto

Tutela delle banche dati

Corte di Giustizia UE, sentenza del 16 luglio 2009 causa C-5/08 - Infopaq International A/S contro Danske Dagablades Forening:

- il diritto d'autore trova applicazione solamente ad un oggetto che abbia carattere di originalità, ossia rappresenti il risultato della creazione intellettuale dell'autore

In aggiunta alla tutela assicurata dal diritto di autore è prevista una forma di tutela denominata diritto 'sui generis' o diritto connesso in base al quale il costitutore di una banca di dati si vede riconosciuto il diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini qualitativi o quantitativi, qualora il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo.



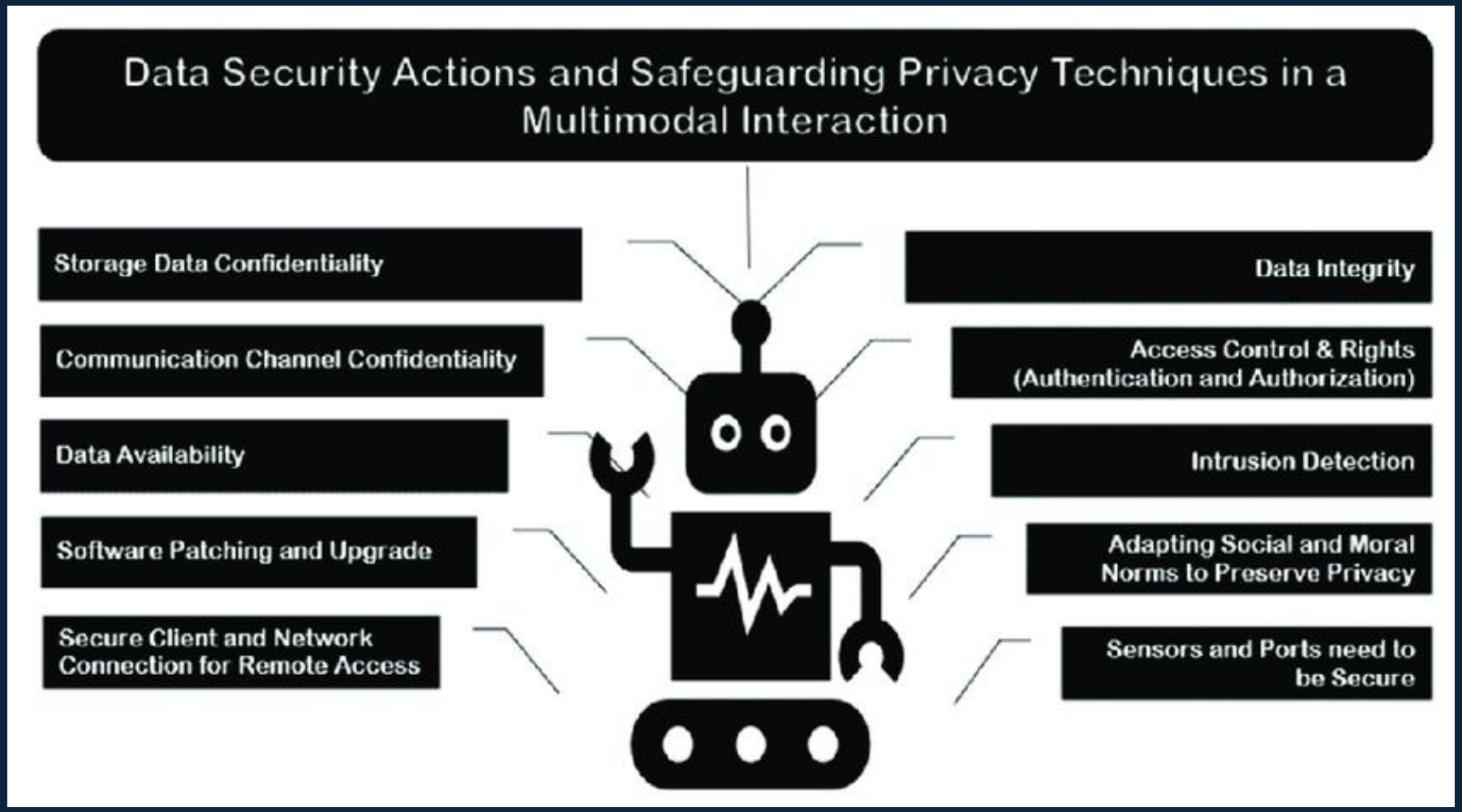
Tutela delle banche dati

In Italia le linee tracciate dalla giurisprudenza di legittimità in merito alla definizione del diritto di autore sono, sostanzialmente, riconducibili a due filoni:

1. reputare come creativa l'opera contenente elementi originali e innovativi che la distinguono da tutte le altre opere

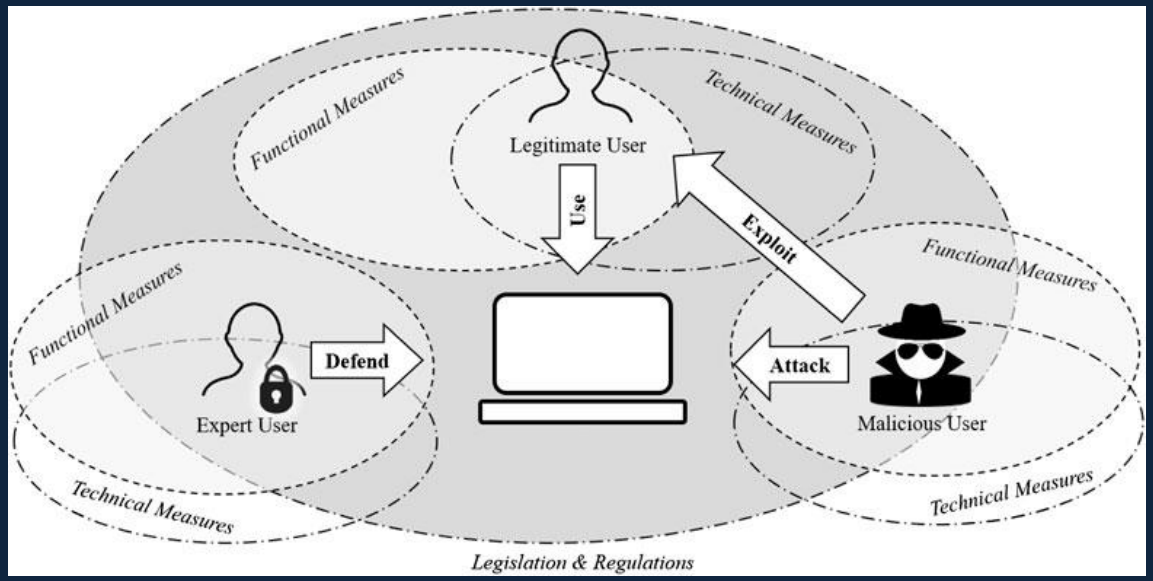
2. reputare creativa l'opera alla quale l'autore abbia conferito una caratteristica tale da personalizzarla

Tutela di software e banche dati



Marchang, Di Nuovo, Multimodal Robotic System (AMRSys): Security and Privacy Issues, Challenges, and Possible Solutions - Applied Sciences

Tutela del capitale umano: protezione del dato personale e tutela della società da cyber attacchi



Governance dei dati

- Governance dei dati = organizzazione e l'implementazione di policies, procedure, strutture, ruoli e responsabilità per una gestione efficace delle risorse informative
- Il Regolamento UE 2016/679 (GDPR) ha introdotto, in aggiunta alla riservatezza propria della privacy, altre due garanzie fondamentali poste a tutela della sicurezza del trattamento: la disponibilità e l'integrità dei dati dell'interessato. Ciò comporta la necessità di fornire indicazioni al titolare e responsabile del trattamento al fine di adottare misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio
- Occorre periodicamente effettuare misure e controlli sui processi per rivedere o produrre nuove policy interne e modelli di gestione dei rischi aderenti alle strutture organizzative
- A queste si aggiunge la necessità di effettuare una valutazione d'impatto (DPIA) per identificare e valutare il rischio di identificazione degli individui, con ricaduta significativa su contenuti e configurazioni contrattuali
- Le attività che ne derivano andranno integrate da una costante formazione ed informazione delle organizzazioni, al fine di creare una maggior consapevolezza dei potenziali rischi

Compliance integrata e corporate governance

Corporate Governance = sistema con il quale l'azienda è amministrata -'insieme delle relazioni tra top management, CdA e shareholders, oltre agli altri portatori di interesse

Obiettivo del sistema di governance è dominare responsabilmente il processo di creazione valore, in modo che risponda alle aspettative dei diversi stakeholder

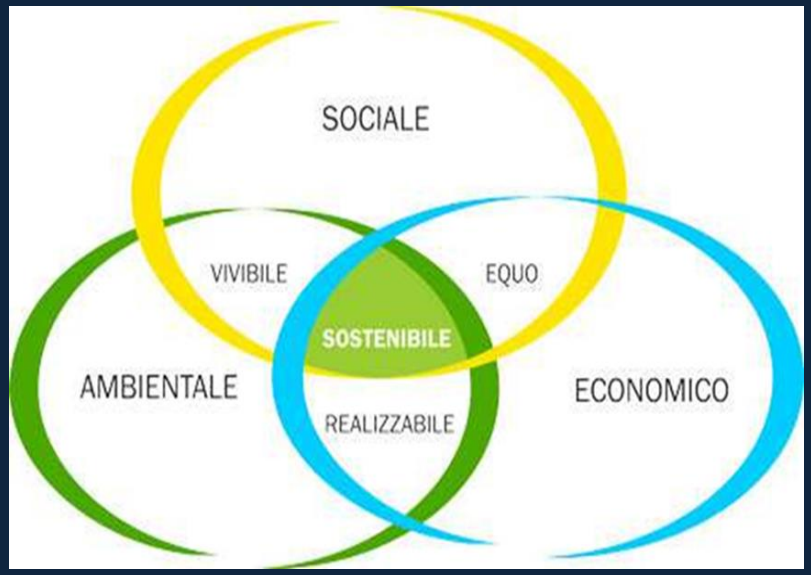
Ai fini di un efficace governance occorre monitorare non solo la compliance, intesa come aderenza alle regole e ai principi interni ed esterni, ma anche la definizione e la misurazione degli obiettivi e delle performance aziendali, l'analisi del rischio, nonché la gestione delle conoscenze e competenze presenti in azienda

Compliance = regole e best practice per guidare il comportamento appropriato del management

Ma le regole da sole non bastano a garantire il buon governo e vanno integrati con meccanismi per la verifica del rispetto delle regole e una cultura che fa del rispetto delle regole un patrimonio comune

In questo modo anche la Corporate Governance entra a far parte del patrimonio immateriale dell'azienda

ESG e sostenibilità aziendale



Custance e Hillier, Statistical issues in developing indicators of sustainable development, Journal of the Royal Statistical Society, 1998

- Anche a seguito della pandemia da Covid-19, le aziende hanno posto maggiore attenzione alla gestione delle risorse immateriali, come il capitale relazionale e il capitale umano e organizzativo, temi ESG fondamentali, nell'ambito della necessaria ridefinizione di prassi e politiche aziendali
- Il bilancio di sostenibilità serve a rendicontare agli stakeholder i risultati economici, sociali e ambientali generati dall'azienda nello svolgimento delle attività
- Ma solo se disponiamo di un sistema di compliance integrata saremo in grado di fornire dati attendibili

Ma questo sarà forse oggetto di un altro convegno …

The End

THANKS FOR YOUR PARTICIPATION !

GRANDE STEVENS
STUDIO LEGALE

GRANDE STEVENS

STUDIO LEGALE

Torino
Via del Carmine, 2
10122 Torino
tel. +39 011 4391411
fax +39 011 4369183/53
torino@grandestevens.it

Milano
Via dell'Annunciata, 7
20121 Milano
tel. +39 02 36 00 92 00
fax +39 02 36 00 92 02
milano@grandestevens.it

Roma
Largo di
Torre Argentina, 11
00186 Roma
tel. +39 06 68413600
fax +39 06 68803124
roma@grandestevens.it