Università
Ca'Foscari
Venezia

Corso di Laurea
Magistrale

in Marketing e
comunicazione
LM-77

Tesi di Laurea

La disciplina dei segreti commerciali come strumento per la tutela del know-how nell'economia digitale

Relatrice
Ch.ma Prof.ssa Alessandra Zanardo

Laureando
Nicola Sartori
Matricola 861284

Anno Accademico
2020 / 2021

Tutti possono vedere le mie tattiche,
nessuno può conoscere la mia strategia.
- Sun Tzu

Tre sono le cose difficili: custodire il segreto,
soffrire le ingiurie, ed impiegare bene il tempo.
- Chilone di Sparta

Due persone possono serbare un segreto
se soltanto una sola lo conosce.
- William Shakespeare

RINGRAZIAMENTI

Durante l'elaborazione di questa tesi di laurea ho avuto modo di collaborare con diversi professionisti attraverso la quale ho acquisito importanti nozioni e conoscenze, risultate poi fondamentali per la stesura di questo testo. Sono stato felicemente colpito nel vedere come esperti del settore dedicavano il loro tempo prezioso ad un semplice studente, sarà questo sicuramente un bel ricordo.

Devo dunque ringraziare la relatrice di questa tesi, la Professoressa Alessandra Zanardo, per l'attenzione dedicata nei miei confronti e per le sue importanti indicazioni che mi hanno permesso di concludere questo lavoro in maniera ottimale. Ringrazio l'Avvocato Stefano Brighenti, per la sua costante e attenta disponibilità nel rispondere alle mie richieste e per la sua cordialità nell'assistermi durante la redazione di questo elaborato. Voglio poi ringraziare l'Avvocato Giovanni Brancalion Spadon, per avermi gentilmente accolto nel suo studio per un confronto sulla tematica *blockchain,* donandomi importanti nozioni sulla materia. Ringrazio l'Avvocato Eugenio Salvatore per avermi offerto degli spunti interessanti su cui riflettere riguardo il futuro della disciplina del segreto, il Dottor Filippo Mazzariol per avermi concesso un'intervista sulla tematica dei diritti di proprietà intellettuale e l'attività di Unioncamere, lo studio commercialista Sarragioto per la consulenza e le informazioni inerenti l'iscrizione a bilancio del segreto commerciale. Infine, ma non meno importante, ringrazio la mia famiglia e gli amici che mi hanno supportato in questi importanti anni di crescita formativa e culturale.

SOMMARIO

INTRODUZIONE

Nell'economia moderna la capacità di generare conoscenza e di trarre benefici da tale conoscenza sta diventando una fonte primaria di vantaggi competitivi, vantaggi che le imprese intendono preservare nel tempo, in quanto questi risultano elementi centrali per l'acquisizione di competenze che permetto di affrontare con maggior successo i mercati economici attuali, caratterizzati da alti livelli di competitività, di velocità e di globalizzazione. Questo elaborato nasce con la volontà di analizzare il segreto commerciale, uno strumento di proprietà industriale che nel corso degli ultimi anni ha acquistato un'importanza rilevante a livello normativo e che si è diffuso in maniera capillare nelle attività d'impresa: questo perché il segreto commerciale ben risponde a quelle che sono le esigenze delle imprese, come la tutela efficace delle conoscenze e la protezione delle informazioni mantenute segrete, siano essi informazioni aziendali o commerciali, o esperienze tecnico-industriali, di natura materiale o immateriale, in particolare nelle piccole e medie imprese (da ora PMI)[1].

L'esigenza di tutelare la segretezza di attività commerciali e mercantili era già presente in età medievale, modellando l'intero sistema economico dell'epoca in rigide corporazioni, chiuse a soggetti e sguardi esterni. La protezione delle conoscenze e delle abilità tecniche da attività di vero e proprio spionaggio industriale permise al ceto mercantile di affermarsi a livello economico, garantendo la riservatezza delle proprie informazioni[2]. Se tuttavia la centralità del segreto può considerarsi una costante nella storia altrettanto non si può dire a riguardo del contenuto della stessa disciplina del segreto. Infatti solo a metà ottocento si riscontrano le prime forme di tutela penale dei segreti commerciali, in particolare in Francia (con i *secret de fabrication*) e poi nel mondo anglosassone (con i *trade secret*), portando lo sguardo oltre la dimensione della fabbrica e della produzione industriale[3]. Queste prime forme di

---

[1] Come indicato da L. VERBAUWHEDE KOGLIN, *"In Confidence". Putting in Place a Trade Secret Protection Program in an SME,* WIPO, 2014, 48, reperibile in internet al seguente indirizzo: https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_amm_14/wipo_smes_amm_14_t5.pdf, le PMI possono trarre vantaggi tangibili dall'utilizzo e dalla comprensione del potenziale valore dei loro segreti commerciali, conseguendo vantaggi competitivi a lungo termine.

[2] Si veda in tal senso R.E. OMODEI, *La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione,* in *Dir. pen. contemp.* 2019, II, 113. Nella letteratura anglosassone si fa spesso riferimento all'attività di spionaggio industriale come *the world's second oldest profession,* ciò dimostrerebbe la diffusione della pratica già in epoca medievale.

[3] Come indicato da R.E. OMODEI, (nt. 2), 113, se la disciplina e il contenuto dei segreti commerciali hanno mutato nel corso dei secoli, la *ratio* sottostante la costituzione della tutela è rimasta quella di garantire all'informazione, alla prassi e alla tecnica la capacità di generare vantaggi competitivi, e quindi un maggiore profitto economico all'imprenditore, mercante o industriale attraverso il mantenimento dello stato di segretezza.

regolamentazione dei segreti commerciali hanno dato vita a casi emblematici[4], come il liquore Chartreuse e la formula della Coca-Cola[5].

L'attuale disciplina italiana in materia deriva, in principio, dall'accordo TRIPS del 1994, ed è stata poi modificata in sede di recepimento dalla direttiva europea sui *Trade secrets*, ampliandone l'applicazione e meglio adattandola alle forme più innovative e tecnologiche di imprese che possiamo trovare nell'economia moderna: le imprese fornitrici di prodotti e servizi digitali. Le imprese che offrono queste tipologie di servizi e prodotti stanno vivendo un forte periodo di crescita dei propri business, questo dovuto principalmente ad una sempre maggiore richiesta, sia da parte del settore privato che del settore pubblico, di mezzi per integrare le loro attività con le ultime tecnologie nel campo digitale, in modo da renderle più efficienti. In aggiunta a ciò sono stati previsti importanti investimenti di risorse pubbliche proprio nell'ambito della digitalizzazione della pubblica amministrazione e delle imprese, come si prefigura essere l'importante piano europeo del *Recovery plan*[6].

Il segreto commerciale può essere ritenuto uno strumento fondamentale per la tutela di valori immateriali che risultano essere, rispetto ai capitali materiali, di più difficile protezione, in particolare l'evoluzione del settore digitale ha permesso alle imprese di disporre di numerose nuove forme di protezione alle proprie informazioni immateriali, queste tecnologie offerte dal settore digitale rendono possibile l'applicazione di protezioni efficienti alle informazioni segrete, le imprese possono così sfruttare in maniera esclusiva il know-how che hanno acquisito nel tempo. Il segreto commerciale diventa perciò un mezzo chiave per la creazione e

---

[4] Il successo di questi primi esempi di segreti commerciali è il risultato del mantenimento della segretezza dei dosaggi, come presentato da D. MASTRELIA, *Gli accordi di trasferimento di tecnologia*, Giappichelli, Torino, 2010, 16, in quanto l'invenzione di un nuovo processo chimico, caratterizzato, ad esempio, da una semplice variazione del dosaggio di un componente, fa ritenere all'impresa più conveniente l'applicazione del segreto commerciale. Ciò è spiegabile in base al rapporto costi/benefici che deriva dalla protezione come segreto rispetto ad altri diritti di proprietà intellettuale, come ad esempio il brevetto, e dal grado di protezione offerto dall'imitazione.

[5] Dall'invenzione di John Pemberton nel 8 maggio 1886 la formula della Coca-Cola è segreta e custodita in una cassaforte nel World of Coca-Cola di Atlanta. La ricetta fu trasferita nell'attuale sede della Coca-Cola nel 2011, in occasione del suo 125° anniversario, fino ad allora era rimasta 86 anni nello stesso cavea della Sun Trust Bank del centro di Atlanta, come indicato nel sito ufficiale Coca-Cola Italia, reperibile in internet al seguente indirizzo: https://www.coca-colaitalia.it/il-nostro-mondo/curiosita/ricetta-segreta.

[6] Il Recovery plan o Next generation EU è un nuovo strumento europeo per la ripresa approvato dal Consiglio europeo straordinario del 21 luglio 2020. I Capi di Stato e di governo europei hanno previsto di incrementare il bilancio su base temporanea tramite nuovi finanziamenti raccolti sui mercati finanziari per un ammontare pari a 750 miliardi di euro (390 miliardi di contributi a fondo perduto e 360 miliardi di prestiti). Il Recovery plan vale per l'Italia circa 248 miliardi, totale complessivo dei progetti e non solamente di quelli previsti da Next Generation EU. Si veda in tal senso Commissione Europea, *Recovery plan for Europe,* https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

la difesa di un vantaggio competitivo nel medio e lungo termine: si vedrà come nelle imprese il capitale sia sempre più costituito da beni intangibili, come esperienze e competenze, processi e codici, liste clienti, tutti elementi che ben si adattano ad essere tutelati con il segreto commerciale, tant'è che la stessa disciplina è stata di frequente causa di sentenze che si sono concluse imponendo anche il pagamento di rilevanti somme di denaro[7].

Sotto il profilo terminologico, tratteremo di segreti commerciali definendoli a volte come informazioni segrete o ancora come informazioni riservate o confidenziali, si menzionerà spesso anche il termine know-how che ne circoscrive una maggiore ampiezza nella definizione; tutti questi termini saranno utilizzati pressoché in maniera indifferente in quanto le presenti espressioni hanno una sostanziale equivalenza nel significato giuridico[8].

La prima parte dello studio si focalizzerà sul tema del segreto commerciale a livello normativo, analizzandone la disciplina sia a livello europeo che a livello italiano, affrontando le modifiche apportate nel corso degli anni che hanno condotto ad una forte evoluzione della materia, nonché analizzando sia i possibili riflessi in bilancio che le fattispecie civilistiche e penali ad esso collegate.

Il secondo capitolo della prima parte confronterà invece le diverse tipologie di proprietà intellettuali, quali il brevetto, il diritto d'autore, modelli d'utilità e disegni e modelli, valutandone le differenze e le rispettive caratteristiche, vagliando la possibilità di integrare questi strumenti e/o cumularli in un sistema per una maggiore tutela delle proprietà industriale, illustrando quali possono essere gli strumenti più adatti per tutelare il capitale di un'impresa a seconda della fattispecie presa in considerazione, approfondendo un caso particolare, qual è il sistema di tutela previsto per i software.

Il terzo capitolo si concentrerà sulle fasi di costituzione di un segreto e sui requisiti che devono essere presenti per assicurare un buon funzionamento dello strumento del segreto commerciale, con possibili campi di applicazione e lo sviluppo di diversi metodi di protezione delle informazioni capaci di garantire il mantenimento dello stato di segretezza.

---

[7] Si veda in tal senso la maxi condanna inflitta ad un manager per una violazione accertata di segreto commerciale dal Trib. Ancona, sez. spec. impresa, 27 maggio 2019, n.1011, in A. GALIMBERTI, *Maxi condanna per segreti industriali violati,* IlSole24Ore, 2019. In questa causa il manager è stato condannato a risarcire 4,5 milioni di euro alla società, una multinazionale tedesca, di cui era stato amministratore delegato e dipendente. La sentenza del Tribunale di Ancona è stato un interessante caso sia per il tema specifico di violazione di segreti commerciali, sia per il metodo di calcolo del danno, che per le ulteriori prescrizioni contro il convenuto, disponendo 100 mila euro di penale per ogni violazione dell'inibitoria.

[8] Ciò è sostenuto anche da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, *La tutela del know-how. Diritto industriale, del lavoro, penale e responsabilità civile,* Giuffrè, Milano, 2012, 62.

La seconda parte analizzerà il tema del segreto commerciale più nello specifico, esaminando come si applica questo strumento attraverso gli strumenti delle imprese digitali e nell'economia c.d. digitale. Si inizierà definendo cos'è oggi un'impresa digitale, quali sono i prodotti che queste imprese offrono al mercato e cosa può determinare, per queste tipologie di imprese, la valorizzazione dell'utilizzo del segreto commerciale, in particolare per il capitale cosiddetto intangibile, e come i strumenti digitali possano essere adeguati per la protezione delle informazioni segrete. Verranno poi approfondite alcune tematiche legate al mondo del digitale che ben si collegano al segreto commerciale per la loro natura o per il loro scopo, come ad esempio la tecnologia *blockchain.* Si vedrà poi come il nuove regolamento europeo sul trattamento dei dati personali ha comportato delle novità alla materia e come la disciplina dei segreti può essere adattata per rispettare tale normativa. Verranno approfondite tematiche quali i *big data,* l'intelligenza artificiale, la *cybersecurity,* l'industria 4.0, tematiche che stanno acquisendo un ruolo centrale per la generazione di conoscenza nelle imprese, valutando possibili applicazioni delle tutele alle informazioni come segreti commerciali, esaminando infine, a termine del quarto capitolo, possibili risvolti pratici per le imprese.

Al termine di questo elaborato verranno presentate delle considerazioni finali sul ruolo attuale e futuro della disciplina del segreto commerciale, indicando alcune possibili modifiche normative che potrebbero interessare l'istituto.

PARTE I

CAPITOLO 1. DISCIPLINA E DEFINIZIONE DEL SEGRETO COMMERCIALE

SOMMARIO: 1.1. Le origini del segreto commerciale - 1.1.1 La Convenzione di Parigi - 1.1.2 L'accordo TRIPS - 1.2. Fonte normative europea: la direttiva UE sui *Trade secrets* - 1.3. Fonte normativa italiana - 1.3.1. L'articolo 98 c.p.i. - 1.3.2. L'articolo 99 c.p.i. - 1.3.3. L'articolo 2598, co. 3, c.c. - 1.4. La tutela penale dei segreti commerciali - 1.5. Riflessi in bilancio.

1.1. Le origini del segreto commerciale

1.1.1. La convenzione di Parigi

Il primo trattato internazionale volto a disciplinare la materia della proprietà intellettuale e industriale fu firmato il 20 marzo 1883 a Parigi, ed è denominato "Convenzione d'Unione di Parigi per la Protezione della Proprietà Industriale". Il trattato fu sottoscritto per la crescente necessità di armonizzare i regolamenti nazionali in ambito di proprietà intellettuale e industriale. L'economia dell'epoca stava vivendo un periodo di forte incremento degli scambi commerciali a livello mondiale, questo principalmente dovuto all'esplosione della seconda rivoluzione industriale, che aveva generato una maggiore globalizzazione dei mercati e nuovi e più efficienti mezzi di comunicazione e trasporto. Era sorta dunque l'esigenza di stabilire regole comuni a livello sovranazionale in tema di marchi, brevetti e modelli industriali per garantire la protezione dei diritti di proprietà industriali ed intellettuale ad imprese che iniziavano a relazionarsi con soggetti provenienti da diverse nazioni del mondo e necessitavo di garanzie di tutela in queste tipologie di rapporti[9].

Sebbene nella Convenzione vengano specificati solamente comportamenti contrari agli usi definiti come onesti in materia industriale e ancora di segreto commerciale non si tratti direttamente, nell'articolo 10-*bis* della Convenzione si può ritrovare una prima forma di tutela di quelli che sono oggi i segreti commerciali all'interno della disciplina più generale della concorrenza sleale, dove si determinava che tra due soggetti vigeva l'obbligo di non divulgare e di non appropriarsi d'informazioni di natura segreta in base a principi di concorrenza leale

[9] Come indicato da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 6 ss.

stabiliti dalla Convenzione[10]. Questo limitava però l'applicazione della tutela a quei rapporti di tipo professionale che potevano determinare l'apprensione, la trasmissione, e l'utilizzazione illecita dei dati segreti, ma non prevedeva ancora nessuna determinazione dei requisiti necessari specifici per valutare un'informazione aziendale come segreto commerciale[11].

1.1.2 L'accordo TRIPS

Solamente con l'accordo TRIPS del 1994 il segreto commerciale viene disciplinato in maniera indipendente e definito per la prima volta a livello mondiale: l'accordo ufficializzato dal GATT[12] al termine dell'incontro avvenuto a Marrakech il 15 aprile 1994 relativo agli aspetti dei diritti di proprietà intellettuale attinenti al commercio[13] è il risultato del negoziato Uruguay Round, l'ottavo ciclo di negoziazioni commerciali in sede GATT, iniziato nel settembre 1986 a Punta del Este (Uruguay), che vede la partecipazione di 123 Paesi e si pone come obiettivo la costituzione di un accordo su tutti gli argomenti più delicati riguardanti le transazioni internazionali, dai dazi sull'agricoltura ai servizi, dalla regolazione della proprietà intellettuale alla questione dell'accesso ai mercati[14].

L'accordo, che vede l'istituzione dell'Organizzazione Mondiale del Commercio (da ora OMC) illustra gli aspetti dei diritti di proprietà intellettuale attinenti al commercio con due obiettivi principali: garantire una protezione efficace e adeguata dei diritti di proprietà intellettuale legati al commercio, tenendo conto delle differenze nei sistemi giuridici

---

[10] Si veda in tal senso P. DI TULLIO, *Commentario breve alle leggi sulla proprietà intellettuale e concorrenza,* a cura di P. MARCHETTI, L.C. UBERTAZZI, Cedam, Padova, 2007, 125, il quale rileva che benché non sia prevista all'interno dell'accordo una disciplina organica relativa propriamente alla concorrenza sleale, è proprio con riferimento alle informazioni segrete che viene operato un riferimento ad essa attraverso il richiamo all'art. 10-*bis* della Convenzione di Parigi. Come indicato anche da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 6 ss. la Convenzione di Parigi del 1883 ha delineato i confini generali del *genus* della concorrenza sleale. Gli stesso autori evidenziano come nella Convenzione comunque mancava una specifica disciplina delle informazioni segrete o riservate, la cui indebita apprensione ed utilizzazione veniva fatta rientrare solo nella disposizione generale dell'art. 10-*bis*.

[11] Bisogna precisare che nella versione iniziale della Convenzione di Parigi non si tratta di concorrenza sleale, questa verrà inserita solamente dall'Aia nel 1925 e integrata fino alla sua forma definitiva nel 1967.

[12] In inglese: *General Agreement on Tariffs and Trade.* Tradotto in italiano: Accordo Generale sulle Tariffe Doganali e sul Commercio.

[13] Applicato dall'UE con decisione 94/800/CE e ratificato dall'Italia con legge 29 dicembre 1994, n. 747.

[14] Si veda Treccani, Dizionario di economia e Finanza, voce *Uruguay Round*, 2012.

nazionali, e la definizione di norme minime multilaterali per combattere la contraffazione[15].

Elementi chiave dell'accordo riguardano il trattamento a livello nazionale ed il trattamento della nazione più favorita, con questo principio tutti i membri dell'OMC devono concedere ai cittadini degli altri stati un trattamento non meno favorevole di quello concesso ai propri cittadini. Oltre a ciò, l'accordo stabilisce che qualsiasi vantaggio concesso da un membro dell'OMC ai cittadini di un altro stato membro dev'essere concesso immediatamente e incondizionatamente ai cittadini di tutti gli altri stati membri dell'OMC.

Nella Sezione 7, all'art. 39 dell'accordo si illustrano le disposizioni inerenti la protezione di informazioni segrete, che, come definito dal co. 1 dell'articolo, devono "*assicurare un'efficace protezione contro la concorrenza sleale ai sensi dell'art.10-bis della Convenzione di Parigi*", si richiama così la regolamentazione generica già stabilita dalla Convenzione di Parigi nel 1967, dimostrando la continuità della materia ma anche la necessità di ulteriori specifiche sull'argomento dei segreti commerciali[16].

È infatti solamente con l'accordo TRIPS che ai membri dell'OMC viene assicurata la protezione delle informazioni e dei dati considerati segreti, in conformità alle indicazioni dei co. 2 e 3 dell'art. 39, dove si illustra che le persone fisiche e giuridiche hanno la facoltà di vietare che, salvo proprio consenso in materia, le informazioni *"sottoposte al loro legittimo controllo*" siano rivelate, acquisite o utilizzate da soggetti terzi in modo contrario a leali pratiche commerciali.

Per l'applicazione della protezione le informazioni prese in esame devono però rispondere a tre determinati requisiti. In primo luogo "*le informazioni devono essere segrete, nel senso che nel loro insieme o nelle loro caratteristiche non sono generalmente note o facilmente accessibili a soggetti che si occupano del tipo di informazione in questione";* inoltre, le stesse *"devono avere un valore commerciale in quanto segrete"* e devono essere *"sottoposte, da parte del legittimo controllore, a misure adeguate, in modo tale da mantenere queste informazioni segrete"*.

All'art. 39, co. 3, si individua una regolamentazione specifica per un determinato settore

---

[15] Si veda il sommario Eur-Lex, *OMC: accordi sugli aspetti della proprietà intellettuale attinenti al commercio,* 2017.

[16] In tal senso anche M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 7, i quali indicano che l'art 39 co. 2 pone un limite alle condotte specifiche di terzi (come rilevazione, acquisizione, utilizzo) in un modo contrario a leali pratiche commerciali, declinando e specificando dunque l'obbligo generale già rinvenibile nell'art. 10-*bis* della Convenzione di Parigi, peraltro espressamente richiamato anche dallo stesso co. 1. art. 39.

riferito come il commercio di prodotti "*chimici farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche",* stabilendo la tutela di dati "*relativi a prove o di altri dati segreti, la cui elaborazione comporti un considerevole impegno, assicurano la tutela di tali dati da sleali usi commerciali"*; questi dati vengono protetti contro la divulgazione, salvo i casi in cui sia necessaria la loro pubblicazione per motivi pubblici, o detta pubblicazione preveda l'attuazione di misure adeguate per garantire la protezione dei dati contro quelli che si considerano usi commerciali sleali. Tale specifica previsione risulta però di poco rilievo, essendo tale tutela già prevista dai co. 1 e 2; probabilmente il legislatore, con tale specificazione, voleva sottolineare la presenza di particolari garanzie in un settore strategico, qual è quello chimico e farmaceutico, contro usi illeciti di informazioni segrete[17].

La matrice dell'art. 39 è chiaramente anglosassone, dato che la terminologia utilizzata è molto vicina a quella adottata dallo *Uniform Trade Secrets Act* americano del 1979. La disposizione sui segreti commerciali risulta essere la più innovativa ma anche contestata dell'accordo TRIPS: tanto è vero che l'art. 39 non si limita a prevedere una mera facoltà ma impone agli stati un vero e proprio obbligo, generando ostilità principalmente dai paesi in via di sviluppo, in particolare in relazione al tema del trasferimento internazionale delle tecnologie[18].

1.2 Fonte normativa europea: la direttiva UE sui *Trade secrets*

L'accordo TRIPS del 1994 prevedeva una prima forma di protezione dei segreti commerciali contro l'acquisizione, l'utilizzo o la divulgazione illecita da parte di terzi, introducendo norme internazionali comuni su quest'aspetto dei diritti di proprietà intellettuale. L'Unione europea stessa, e con essa gli Stati membri, è vincolata da tale accordo, approvato con la decisione 98/800/CE del Consiglio della UE[19].

---

[17] Si veda F. SANNA in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 62. Tale disposizione assume un importante rilievo se si considera la riluttanza di molti ordinamenti ad accogliere sistemi di protezione temporalmente allungata in relazione al settore farmaceutico e chimico. Si veda in tal senso il caso DuPont contro la Kolon Industries, in cui la Kolon, e molti dei suoi dirigenti e dipendenti, sono stati incriminati per un coinvolgimento in una campagna pluriennale sviluppata con il fine ultimo di acquisire segreti commerciali relativi alla fibra para-aramidica Kevlar di DuPont. La Kolon Industries è stata dichiarata colpevole di un'accusa federale per acquisizione illecita di segreti commerciali, per la quale è stata disposta una sanzione penale di 85 milioni di dollari, come indicato da L. VERBAUWHEDE KOGLIN, (nt. 1), 5.

[18] In tal senso si è espressa F. SANNA in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 59, la norma, infatti, ha reso più difficile e costoso l'accesso alle informazioni di carattere tecnologico, inoltre, la disciplina fa riferimento in particolare proprio a due settori estremamente importanti per l'economia dei paesi in via di sviluppo: il settore agricolo e quello farmaceutico.

[19] Decisione 94/800/CE del Consiglio Europeo del 22 dicembre 1994 sugli accordi dei negoziati multilaterali dell'Uruguay Round (1986-1994).

L’attuale disciplina italiana sul segreto commerciale è un’attuazione però della direttiva UE 2016/943 del Parlamento Europeo e del Consiglio dell’8 giugno 2016, sulla protezione del cosiddetto know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione in maniera illecita.

La direttiva UE 2016/943 (da ora la direttiva) si colloca all’interno di una azione strategica della Commissione atta a rinforzare gli strumenti di difesa della proprietà intellettuale, in quanto fonte dell’economia della conoscenza e fornitrice di vantaggi competitivi per le imprese. Per segreto commerciale s’intende il patrimonio di know-how e di informazioni di natura commerciale non divulgate e destinate a rimanere segrete[20].

La riservatezza delle informazioni dell’impresa risultava essere sempre più uno elemento fondamentale per la competitività commerciale, per la gestione dell’innovazione nel settore della ricerca e per l’acquisizione di valore delle informazioni di natura tecnologica o commerciale. Si rendeva pertanto necessario definire con precisione le informazioni meritevoli di tutela, quali i segreti industriale, in quanto potevano essere di diverso tipo, come, ad esempio: dati sui clienti e fornitori, piani aziendali, ricerche e strategie di mercato.

L’economia moderna è caratterizzata da un’espansione delle tecniche di *open innovation*[21], tecniche che hanno permesso alle imprese di ampliare la quantità e la qualità delle relazioni con soggetti esterni, permettendo una maggiore diffusione delle conoscenze e delle informazioni, assicurando peraltro l’opportunità di uno sviluppo dinamico, efficiente ed equo, in particolare per le PMI. Si è resa pertanto necessaria l’adozione di strumenti in grado di tutelare lo scambio di conoscenze tra soggetti ed organizzazioni, sia nel mercato interno che extraeuropeo, generando un contesto più ottimale per le attività di ricerca e sviluppo e dell’innovazione. Infatti, aumentando le relazioni esterne le imprese sono più esposte a pratiche che possiamo definire fraudolente, come copie non autorizzate, furto, spionaggio

---

[20] Valutando l’impatto del recepimento della direttiva sull’ordinamento italiano S. SERAFINI, *Luci ed ombre della nuova disciplina sul segreto commerciale,* in *Corr. giur*., 2018, XI, 1330, dichiara che l’impatto del recepimento della direttiva da parte dell’ordinamento italiano deriva innanzitutto dalla conferma dell’avvicinamento dello standard di tutela accordato al segreto allo schema delle privative. La circostanza di questo rafforzamento di tutela si applica anche alle informazioni di carattere meramente commerciale, come ad esempio le tecniche di marketing, le liste clienti profilate etc., oltre a quelle di carattere puramente innovativo o legate all’esperienza tecnica. In tal senso si veda anche il considerando 1 della direttiva.

[21] L’open innovation è un approccio all’innovazione sostenuto da imprese che producono idee, risorse e competenze tecnologiche attraverso la collaborazioni con soggetti e organizzazioni esterne, in particolare modo con startup, università, enti di ricerca, fornitori e consulenti. Il termine, che significa “innovazione aperta”, è stato coniato dall’economista statunitense H. CHESBROUGH, come precisato nel saggio *The era of open innovation,* 2003.

economico o violazione degli obblighi di riservatezza, da parte di soggetti ed organizzazioni con origine sia europea che al di là dei confini dell'Unione. Altri sviluppi recenti, quali la globalizzazione, un maggior ricorso all'esternalizzazione della produzione, catene di approvvigionamento più lunghe e strumenti della comunicazione e informazione più diffusi, tendono ad aumentare il rischio per le imprese di essere vittime di pratiche fraudolente, disincentivandole ad aprirsi maggiormente a mercati stranieri per lo sviluppo di attività transfrontaliere, mettendo a serio rischio il diffondersi delle pratiche di *open innovation*.

Da una consultazione pubblica, svoltasi tra il 2012 e il 2013 e che ha coinvolto quasi tutti gli Stati membri dell'Unione europea, è emersa la necessità di fornire una tutela del segreto commerciale maggiore e più uniforme tra tutti gli Stati membri per rispondere alle esigenze sopra menzionate. Nonostante la sottoscrizione dell'accordo TRIPS, in Europa si rilevavano infatti ancora numerose differenze nelle normative nazionali degli Stati membri per la regolamentazione dei segreti commerciali contro l'acquisizione, l'utilizzo o la divulgazione illecita da parte di terzi. Non tutti gli Stati membri avevano infatti adottato definizioni nazionali di segreto commerciale, non vi era coerenza per quanto riguardava gli strumenti di tutela ed esistevano anche notevoli differenze nelle regolamentazioni per ciò che disciplinava il trattamento di un terzo soggetto, acquirente di un segreto commerciale in buona fede. Le norme tra i diversi paesi UE differivano anche per ciò che trattava la facoltà, per i legittimi detentori dei segreti commerciali, di chiedere la distruzione delle merci prodotte da terzi, quali soggetti utilizzatori in modo illecito di segreti commerciali; un'ulteriore importante differenza si riscontrava sulle norme per il calcolo dei danni, determinando trattamenti diversi all'interno dell'Unione[22].

Tutte queste importanti differenze nelle legislazioni nazionali degli Stati membri causavano l'applicazione di livelli di protezione differenziati all'interno dell'Unione, le imprese erano così scoraggiate nell'intraprendere attività economiche all'estero per lo sviluppo d'innovazioni, compresa la cooperazione con partner europei in materia di ricerca e sviluppo, produzione, esternalizzazione e/o investimenti. Ciò poteva comportare un'allocazione inefficiente dei capitali destinati alle attività innovative, facilitando l'importazione

---

[22] In tal senso si vedano le premesse della direttiva, par. 6,7,8. Si veda anche V. FALCE, *Tecniche di protezione delle informazioni riservate. dagli accordi Trips alla Direttiva sul segreto industriale,* in *Dir. ind.*, 2016, III, 129, dove si precisa che gli accordi TRIPS scolpiscono principi e regole generali che tuttavia sono state trasfuse a livello nazionale in regolamenti sostanziali e procedurali che risultano però anche notevolmente disomogenei.

nell'Unione e il diffondersi di comportamenti di concorrenza sleale. Il rischio era così di consentire l'ingresso di merci provenienti da paesi terzi con livelli di protezione inferiori, ma frutto di una progettazione, una produzione e una commercializzazione che sfruttava segreti commerciali acquisiti in maniera illecita[23].

La direttiva ha permesso di equilibrare la disciplina dei segreti commerciali tra gli Stati membri, ovviando a queste differenze e questi problemi, lasciando comunque la facoltà agli Stati membri di fornire un livello di protezione più amplio dei segreti commerciali, sempre nel rispetto delle garanzie previste dalla direttiva per la protezione degli interessi delle diverse parti.

La direttiva, come previsto all'art. 1, è stata redatta nel rispetto delle disposizioni del TFUE e delle norme dell'Unione o dei singoli Stati membri che prevedono la divulgazioni di informazioni, inclusi i segreti commerciali, al pubblico o alle autorità in caso di specifiche esigenze, senza quindi bloccare il normale svolgimento delle attività di autorità pubbliche per il controllo o l'informazione al pubblico in caso di reati, garantendo sempre l'accesso del pubblico a documenti o agli obblighi di trasparenza.

La direttiva garantisce inoltre i diritti delle parti sociali per la stipulazione di accordi di tipo collettivo o per la difesa collettiva degli interessi dei lavoratori, non prevedendo nessuna giustificazione nel limitare la libertà dei dipendenti[24], garantisce inoltre il diritto all'informazione, per quanto concerne il giornalismo d'inchiesta e la protezione delle fonti giornalistiche, compreso il rispetto delle libertà e del pluralismo dei media, nell'esercizio

---

[23] In tal senso si è espresso A. OTTOLIA, *Il D.lgs. n. 63/18 di attuazione della dir. 2016/943/UE sulla protezione dei segreti commerciali fra tutela e bilanciamenti*, Le Nuove Leggi Civili Commentate, Cedam, 2019, 1091, indicando che la disciplina di armonizzazione europea sulla protezione delle informazioni commerciali riservate contenuta nella direttiva è stata realizzata per conseguire un avvicinamento moderato tra le diverse discipline nazionali, le cui differenze erano peraltro compatibili con la tutela minima garantita nell'accordo di TRIPS, ma che invece non aveva determinato l'introduzione di un titolo unitario nella UE. La direttiva è stata così adottata a seguito dell'esplicita presa d'atto da parte della stessa Commissione europea che il segreto commerciale rappresenta uno strumento complementare alle altre forme di tutela della proprietà industriale e intellettuale. Le diversità riscontrate tra le discipline nazionali in questo ambito potevano infatti costituire un serio ostacolo allo sviluppo del Mercato Unico europeo.

[24] E' questo un aspetto particolarmente rilevante, si veda a tal senso App. Perugia, sez. lavoro, 10 gennaio 2020, in *DeJure*, in cui, trattando il tema della fidelizzazione del dipendente, si evidenzia come la direttiva sulla protezione del know-how riservato e delle informazioni commerciali riservate contro l'acquisizione, l'utilizzo e la divulgazione illeciti si ispira al medesimo e importante principio di tutela del lavoro, sul quale si è fondato l'insegnamento del giudice di legittimità: nessuna disposizione prevista dalla direttiva è da intendersi infatti come giustificazione per limitare la mobilità dei dipendenti. In particolare, in relazione all'esercizio del diritto di mobilità, la direttiva non offre giustificazioni per: limitare l'utilizzo, da parte dei dipendenti, di informazioni che non costituiscono un segreto commerciale o limitare l'utilizzo, da parte sempre dei dipendenti, di esperienze e competenze acquisite in maniera onesta nel normale svolgimento del proprio lavoro.

della libertà di espressione e d'informazione, come precisato nell'art. 11 della Carta dei diritti fondamentali dell'Unione europea. In linea con il principio di proporzionalità, gli strumenti di tutela dei segreti commerciali sono stati adeguati in modo tale da permettere il raggiungimento dell'obiettivo di un corretto funzionamento del mercato interno europeo, sostenendo investimenti per la ricerca e l'innovazione, senza però compromettere o minare, allo stesso tempo, i diritti e le libertà fondamentali stabiliti dall'interesse pubblico, o limitare la possibilità di denunciare delle irregolarità; conferendo, infine, alle autorità giudiziarie il potere di adottare misure adeguate relativamente ai richiedenti, in particolare nel caso di richiedenti che agendo in mala fede o in modo illecito presentavano denunce infondate con l'obiettivo ultimo di ritardare o limitare l'accesso del convenuto al mercato, ostacolando così la libera concorrenza nel settore. Proprio per questo motivo è stata prevista la possibilità di applicare la protezione dei segreti commerciali solo per un periodo limitato, in base alle disposizioni determinate dal diritto nazionale[25].

Nell'art. 2 della direttiva vengono definiti i requisiti necessari affinché un'informazione sia assoggettata alla disciplina del segreto commerciale, in linea con quelle che sono le disposizioni degli accordi TRIPS. Sono definiti segreti commerciali le informazioni che presentano certe caratteristiche, quali la segretezza, "*nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione*; le informazioni devono inoltre presentare elementi che ne implichino un certo "*valore commerciale in quanto segrete"* ed infine tali informazioni devono essere "*sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette a mantenerle segrete"*. I tre requisiti che determinano le caratteristiche del segreto commerciale possono essere quindi sintetizzati in informazioni che non sono note o diffuse tra il pubblico, hanno un valore economico intrinseco data la loro particolare natura segreta e vedono l'attuazione di misure adeguate per mantenere queste informazioni segrete.

Si è inoltre definito nella direttiva con maggiore precisazione che sia il detentore che l'autore della violazione possono essere persone sia fisiche che giuridiche e che per violazione s'intende l'acquisizione, l'utilizzazione o la divulgazione del segreto commerciale in una

[25] In tal senso si veda la definizione del principio di proporzionalità che è esposto al considerando 21 della direttiva.

maniera illecita. L'acquisizione illecita di un segreto commerciale può avvenire quando è frutto di un accesso non autorizzato, con appropriazione di copie, documenti, oggetti, materiale, sostanze o file elettronici nel legittimo controllo del detentore del segreto commerciale o in qualsiasi altro modo contrario alle leali pratiche commerciali. L'utilizzo o la divulgazione illecita possono venire determinati da un'acquisizione illecita del segreto, dalla violazione di un accordo di riservatezza o di un qualsiasi altro obbligo legale, dalla violazione di un obbligo contrattuale o di altra natura che limiti l'utilizzo del segreto commerciale[26]. Ulteriormente a ciò, l'acquisizione, l'utilizzo o la divulgazione sono da considerare illeciti nel caso in cui, secondo precise circostanze, il soggetto avrebbe dovuto essere a conoscenza del fatto che il segreto commerciale era stato ottenuto da un terzo, il quale l'aveva acquisito a sua volta in maniera illecita, in maniera diretta o indiretta. La valenza del segreto commerciale si estende anche nel caso in cui la produzione, l'offerta o la commercializzazione oppure l'importazione, l'esportazione o lo stoccaggio di merci sono frutto di un utilizzo illecito del segreto commerciale, costituendone una violazione.

Nella direttiva, all'art. 3, vengono anche definite una serie di possibili azioni di acquisizioni, utilizzo e divulgazione di segreti commerciali considerate lecite. Questi casi comprendono: la modalità di scoperta o la creazione definita indipendente, o altrimenti tramite lo studio, smontaggio, osservazione o prova di un prodotto o di un oggetto che risulti a disposizione pubblica o lecitamente in possesso di chi acquisisce le informazioni (c.d *reverse engineering*). Il soggetto che acquista in maniera lecita queste informazioni dovrà essere però in ogni caso libero da ogni obbligo giuridico valido da imporre restrizioni all'acquisto di segreti commerciali[27].

---

[26] Art. 4 direttiva UE 2016/943. Si veda anche V. FALCE, *Dati e segreti. Dalle incertezze del Regolamento Trade secret ai chiarimenti delle Linee Guida della Commissione UE,* in *Dir. ind.,* 2018, II, 157, dove si indica che nell'art. 4 della direttiva si elencano le condotte di acquisizione, divulgazione e utilizzazione illecita di informazioni riservate, per poi rimettere ad una previsione di chiusura (nel co. 2, lett. b, art. 4) la precisazione che ogni condotta difforme dal paradigma dell'*unfair competition* è illegittima e dunque vietata.

[27] Il *reverse engineering* è un processo di analisi effettuato attraverso supporti informatici, per lo studio di forme e di comportamenti di un oggetto, tecnico o biologico, allo scopo di analizzarne il funzionamento e poterlo eventualmente riprodurre per poi migliorarlo, ricostruendone il progetto alla base. A riguardo si veda Treccani, voce *reverse engineering,* 2008. Si veda anche V. FALCE, (nt. 26), 157, in cui si approfondisce la tematica dell'art. 3 che, per converso, e anche in un'ottica di armonizzazione e di convergenza, contiene le condotte lecite che vengono presentate in via esemplificativa, con la dovuta precisazione che sono legittime solamente quelle attività in cui il medesimo risultato informativo è frutto di processi di decompilazione o anche espressione di possibili coincidenze fortuite. Si veda inoltre G. GHIDINI, G. CAVANI, *Proprietà intellettuale e concorrenza. Corso di diritto industriale*, Torino, Zanichelli, 2021, 36, in cui si specifica che se l'attività di decompilazione è realizzata senza particolari difficoltà da un parte di soggetto esperto del settore, questo esclude la natura riservata delle informazione, non essendo state adottate misure adeguate a mantenere la riservatezza.

All' art. 5 vengono precisate una serie di "eccezioni" alla tutela, costituendo un sistema di bilanciamento con altri interessi e diritti che potrebbero interferire con il segreto[28]. Si prevedono perciò una serie di modalità di acquisizione lecita dei segreti commerciali, come nel caso di esercizio del diritto di informazione o di espressione, compreso il rispetto della libertà e del pluralismo dei media, nella rilevazione di una condotta scorretta per la denuncia di un'attività irregolare o illecita in modo tale da proteggere l'interesse pubblico o in fasi di consultazione da parte di lavoratori o rappresentanti dei lavoratori in attuazione dei diritti fondamentali già illustrati precedentemente; possono infine venir considerate lecite le pratiche di acquisizione di segreti commerciali conformi a leali pratiche commerciali, che vanno però valutate secondo le circostanze.

Importante è stata la determinazione, nella direttiva, dei sistemi di tutela volti a garantire la riservatezza del segreto commerciale oggetto di un contenzioso nel corso di procedimenti giudiziari[29]. Tra queste figura la possibilità di limitare la cerchia di persone autorizzate ad aver accesso alle prove e agli atti delle udienze, assicurando, pertanto, la tutela della riservatezza dei segreti commerciali e il rispetto dei diritti delle parti per un processo che sia equo e con una tutela effettiva. La prospettiva di una perdita della riservatezza dei segreti commerciali durante un processo infatti può scoraggiare i legittimi possessori del diritto dall'avviare procedimenti per la tutela di suddetti diritti di proprietà industriale. La protezione del segreto commerciale dev'essere quindi garantita durante tutta la pendenza del processo e anche nelle fasi successive, fino a quando le informazioni contenute nel segreto non diventeranno di dominio pubblico. Si è così determinato che i soggetti legittimati ad aver pieno accesso alle prove o alle udienze saranno una cerchia ristretta di persone, e dovranno comprendere almeno una persona fisica per ogni parte in causa e i rispettivi avvocati o di altri rappresentanti adeguatamente qualificati ai sensi del diritto nazionale per difendere, rappresentare, servire gli interessi di una parte nel processo.

La direttiva ha previsto una serie di misure provvisori leali, eque, efficaci e dissuasive per il

---

[28] Come sostenuto da A. OTTOLIA, (nt. 23), 1121, in cui si illustra una serie di linee interpretative, dove si fa preciso riferimento a diverse ipotesi di bilanciamento contenute all'art. 5 della direttiva. L'autore però precisa che tale disposizione non è utile a individuare la tipologia di bilanciamento da porre in essere, dato che l'art. 5 della direttiva, dove sono indicate le "eccezioni" alla tutela, contiene già bilanciamenti unilateralmente cristallizzati a favore di alcuni interessi puntuali nei casi di interferenze con la disciplina del segreto commerciale.

[29] Art. 9 Direttiva UE 2016/943. Si vedano anche i considerandi 25 e 26 della direttiva.

blocco di eventuali acquisizioni, utilizzi e divulgazioni illecite di un segreto commerciale, anche da parte di terzi soggetti[30]. Questo si è reso necessario in quanto in caso di divulgazione pubblica del segreto per il detentore diverrebbe impossibile tornare alla situazione precedente alla perdita del segreto, determinandone un forte danno, le stesse informazioni potrebbero infatti essere utilizzate illecitamente per progettare, produrre o commercializzare merci e componenti con l'obiettivo di distribuirli e venderli nel mercato interno dell'Unione, provocando un impatto negativo sui traffici commerciali del detentore del segreto. Sono state perciò introdotte una serie di disposizioni che concedono alle autorità giudiziarie strumenti efficaci e appropriati al fine di garantire che tali prodotti non siano immessi nel mercato e vengano prontamente ritirati nell'intera Unione. Misure, procedure e strumenti di tutela devono essere proporzionati, tali da evitare la creazione di ostacoli e prevedere garanzie contro gli abusi, come stabilito dall'art. 7 della direttiva. La determinazione della prescrizione è stata demandata al diritto degli Stati membri ma viene indicato che non deve in ogni caso superare i sei anni.

La direttiva ha indicato una regolamentazione specifica anche nel caso di acquisizione inizialmente in buona fede del segreto commerciale, ma che poi è mutata, a causa della conoscenza da parte del terzo soggetto dell'utilizzazione in una maniera che è da considerare illecita. Al fine di evitare misure correttive sproporzionate, la direttiva prevede che l'indennizzo non superi i diritti dovuti qualora il soggetto interessato avesse ottenuto l'autorizzazione ad utilizzare il segreto commerciale.

Riguardo la decisione giudiziaria, in presenza di una decisione adottata nel merito, le competenti autorità giudiziarie possono prevedere eventuali misure come la cessazione o il divieto di utilizzo o divulgazione del segreto commerciale, il divieto di produzione, offerta, commercializzazione o utilizzazione delle merci costituenti violazione con l'applicazione di adeguate misure correttive come possono essere il richiamo dal mercato, l'eliminazione, la distruzione o il ritiro di queste tipologie di merci con possibile consegna al detentore del segreto commerciale o ad associazioni a scopo benefico[31]. La sentenza può prevedere anche la distruzione totale o parziale dei documenti, oggetti, materiali, sostanze che incorporano il

---

[30] Art. 6 direttiva UE 2016/943.

[31] Art. 12 direttiva UE 2016/943. In tal senso si veda A. CHIABOTTO, *La protezione dei segreti commerciali: la direttiva UE 2016/943,* in *Contr. impr. Eur,* 2016, II, 785 ss.

segreto commerciale. Nel caso di un utilizzo illecito di un segreto commerciale la direttiva sottolinea anche la necessità di prevedere un risarcimento del danno alla parte lesa con un importo che dovrà tener conto di tutti i fattori pertinenti, quali il lucro cessante subito dal detentore del segreto o i profitti realizzati ingiustamente dal detentore illegittimo del segreto, possono anche essere ulteriormente aggiunti nel calcolo i danni morali arrecati al detentore del segreto commerciale. Come già accennato, in caso di difficoltà riscontrate nel calcolare l'importo, è prevista la possibilità di determinare il totale in base ai diritti che sarebbero stati dovuti se l'autore della violazione avesse richiesto l'autorizzazione per l'utilizzo del segreto commerciale. Il risarcimento dovrà in ogni caso essere fondato su una base oggettiva, tenendo conto di tutte le spese sostenute dal detentore del segreto commerciale, come i costi legati all'individuazione della violazione e delle relative ricerche[32].

La direttiva prevede anche la possibilità che la sentenza possa essere pubblicata tramite mezzi di pubblicità a grande diffusione in relazione ai procedimenti che specificano l'acquisizione, l'utilizzo o la divulgazione in maniera illecita di segreti commerciali, garantendo tuttavia che tale pubblicazione non comporti la diffusione del contenuto del segreto. Vengono infine indicate misure provvisorie e cautelari da applicare nei confronti del presunto autore della violazione: dalla cessazione o divieto di utilizzo provvisorio del segreto, al divieto di produzione, offerta, commercializzazione o utilizzazione di merci costituenti violazione, con possibile sequestro e/o consegna di queste merci[33].

---

[32] Art. 14 direttiva UE 2016/943. Si veda anche A. CHIABOTTO, (nt. 31), 786 ss., dove si precisa l'esistenza di un sistema "binario" di percorsi alternativi per il risarcimento danni. Nel caso di violazione consapevole o colposamente inconsapevole, il titolare infatti può optare: in primo luogo per una liquidazione, dove si valutano tutti gli aspetti pertinenti, quali le conseguenze economiche negative, compreso il mancato guadagno subito dalla parte lesa, ed i benefici realizzati illegalmente dall'autore della violazione, in aggiunta, nei casi appropriati, possono inserirei ulteriormente elementi diversi da quelli economici, come il danno morale arrecato al titolare del diritto dalla violazione del medesimo. Oppure, una seconda modalità di valutazione può essere scelta dal titolare, qualora non si opti per la soluzione della liquidazione, determinando il danno applicando un metodo di quantificazione calcolato in misura forfettaria, tenendo conto, per lo meno, dell'importo che avrebbe dovuto essere riconosciuto al titolare qualora l'autore della violazione avesse richiesto l'autorizzazione per l'uso del diritto di proprietà intellettuale in questione.

[33] Art. 10 direttiva UE 2016/943. In tal senso A. CHIABOTTO, (nt. 31), 784 ss., precisa che la direttiva offre un rimedio alla situazione preesistente che presentava un'incoerenza tra gli strumenti di tutela di natura civile disponibili in caso di acquisizione, utilizzo o divulgazione illecita di segreti commerciali all'interno della UE, e alla mancanza della possibilità di ricorrere, in tutti gli Stati membri, a ordini di cessazione e astensione contro eventuali terzi soggetti, che non rivestano la qualifica di concorrenti diretti del legittimo detentore del segreto. Perciò l'art. 10 della direttiva ha previsto esplicitamente la possibilità, per il detentore del segreto commerciale, di rivolgersi all'autorità giudiziaria in modo tale da ottenere misure provvisorie e cautelari nei confronti del presunto autore della violazione, anche nel caso in cui quest'ultimo non sia un concorrente diretto.

1.3. Fonte normativa italiana

L'Italia aveva già adeguato il proprio ordinamento giuridico alle protezioni minime stabilite dal modello comune dell'accordo TRIPS del 1994, prima tramite l'art. 6-*bis* della Legge Invenzioni, che disciplinava l'ipotesi dell'abuso del segreto come fatto lesivo del diritto alla lealtà della concorrenza. L'art. 6-*bis* della Legge Invenzioni è stato poi abrogato con l'introduzione del Codice della Proprietà Industriale (da ora c.p.i.) che ne ha trasfuso il contenuto agli artt. 98 e 99, ricomprendendo il segreto nell'ambito della proprietà industriale sebbene diritto non titolato, in quanto acquisito senza necessità di un specifico procedimento[34]. In attuazione della direttiva UE 2016/943 del Parlamento europeo e del Consiglio dell'8 luglio 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illecita è stato emanato il decreto legislativo 11 maggio 2018 n. 63 (da ora il decreto) che ha apportato talune modifiche al c.p.i. e al codice penale, introducendo una disciplina specifica concernente *l'enforcement* processuale, adeguando la normativa italiana a quella della UE[35].

In *primis* vengono sostituite nel c.p.i. le parole "informazioni aziendali riservate" applicando all'intero testo la definizione di "segreto commerciale"[36], vengono modificati gli artt. 98 e 99 c.p.i. aggiornandoli con le disposizioni della direttiva UE, vengono inoltre stabilite delle

---

[34] Si veda il d.lgs. 10 febbraio 2005, n. 30 Codice della Proprietà industriale, a norma dell'art. 15 della legge 12 dicembre 2002, n. 273. Per una maggiore trattazione della nuova disciplina introdotta con il d.lgs. n. 30 del 2005 si veda S. SERAFINI, (nt. 20), 1331, in cui si sostiene che l'ambito della tutela nella disciplina del c.p.i diviene molto ampio, in quanto l'oggetto della tutela sono tutte le possibili informazioni aziendali, le esperienze tecnico-industriali, comprese quelle di natura commerciale; la privativa in questione può così riguardare sia il c.d. know-how, costituito dal patrimonio delle conoscenze pratiche e non brevettate acquisite con esperienze e prove, sia le informazioni meramente commerciali. Si veda anche P. AUTERI, *Diritto Industriale, proprietà intellettuale e concorrenza*, Torino, Giappichelli, 2020, 209.

[35] Il d.lgs. è stato pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana il 7 giugno 2018. Si veda S. SERAFINI, (nt. 20), 1333, dove trattando le novità introdotte con il d.lgs. 11 maggio 2018 n. 63 si esplicita che sebbene ad una prima impressione, leggendo le novità introdotte dal d.lgs. al c.p.i., non si riscontrino modifiche sostanziali e importanti, si introduce piuttosto una disciplina specifica concernente *l'enforcement* processuale, adeguandola con la normativa prevista dalla UE.

[36] La sostituzione terminologica ha interessato gli art. 1, co.1 e art. 2, co. 4 c.p.i., come indicato da G. GHIDINI, G. CAVANI, (nt. 27), 38. In tal senso si veda A. OTTOLIA (nt. 23), 1094, trattando l'ambito soggettivo della tutela sottolinea che il cambiamento apportato al c.p.i. ha una valenza pressoché interpretativa, tant'è che la sostituzione dell'espressione "informazioni aziendali riservate" con quella di "segreto commerciale", nel capo primo del codice dedicato alle definizioni e ai principi generali, induce a ritenere che l'aggettivo "commerciale" non sia da considerarsi come sinonimo di "aziendale" ma si trovi in un rapporto di "genere" e di "specie" con quest'ultimo. Infatti il termine "aziendale" implica una "provenienza", nonché una determinata strumentalità, secondo lo schema dell'art. 2555 c.c. L'aggettivo invece "commerciale" determina più in generale un'idoneità dell'informazione a essere utilizzata nel mercato. Questa precisazione si collega necessariamente al tema dei soggetti tutelabili, che non sembrano più dunque limitati a solo coloro che svolgono un'attività economica d'impresa. Come evidenziato da A. OTTOLIA ciò ha comportato un'estensione soggettiva della tutela, consentendo, anche al soggetto non imprenditore, di avvalersi del segreto commerciale.

disposizioni per la tutela della riservatezza dei segreti commerciali nel corso di procedimenti giudiziari, praticando dei cambiamenti all'art. 121-*ter* c.p.i., quali il divieto imposto dal giudice di rivelare segreti commerciali od oggetti del procedimento ritenuti riservati in capo a soggetti nominati dal giudice o delegati, dalle parti o dai loro rappresentanti, dal personale amministrativo, dai testimoni e difensori e da qualunque altro soggetto che ha accesso ai provvedimenti, agli atti o ai documenti presenti nel fascicolo.

Viene stabilito che il provvedimento di divieto, pronunciato inizialmente su istanza di parte, mantiene efficacia anche successivamente alla conclusione del procedimento, perdendola invece in caso di sentenza passata in giudicato con accertamento di segreti commerciali privi dei requisiti previsti o in caso di segreti commerciali diventati generalmente noti o facilmente accessibili. Si attribuisce al giudice la facoltà di attuare tutti i provvedimenti idonei a tutelare la riservatezza dei segreti commerciali, come la limitazione ad un numero ristretto di soggetti dell'accesso alle udienze e agli atti dei documenti, l'oscuramento, l'omissione delle parti contenenti segreti commerciali, la diffusione di copie del provvedimento con parti oscurate od omesse ed il divieto per le parti di diffondere il provvedimento in versione integrale, tutto ciò in attuazione dell'art. 9 della direttiva UE 2016/943[37].

Il decreto ha previsto delle ulteriori modifiche anche sul piano sanzionatorio all'art. 124 c.p.i., prevedendo che il giudice nel corso di procedimenti relativi alla violazione di un segreto commerciale dovrà disporre di misure proporzionate a seconda del valore, delle caratteristiche specifiche, delle misure adottate dal legittimo detentore per la tutela del segreto, della condotta dell'autore, dell'impatto dell'utilizzazione o della rivelazione dei segreti

---

[37] Come disposto dall'art. 5 d.lgs. 63/18. Si veda anche S. SERAFINI, (nt. 20), 1334 che precisando le novità introdotte dal decreto, sottolinea come le previsioni del nuovo art. 121-*ter* c.p.i., abbiamo previsto un'apposita disciplina a tutela della riservatezza dei segreti commerciali nei procedimenti giudiziari, la quale permetterebbe al giudice, su istanza di parte, di vietare l'acquisizione, la rivelazione e l'utilizzo dei segreti oggetto del giudizio a soggetti come consulenti, difensori, personale amministrativo etc. che hanno accesso al fascicolo giudiziario. Questo con lo scopo specifico di tutelare la segretezza delle informazioni. Il giudice può inoltre limitare l'accesso al fascicolo, ordinando l'oscuramento di parti dei provvedimenti che definiscono il giudizio. L'autore sottolinea le notevoli novità che hanno interessato l'apparato processuale relativo al segreto commerciale, per cui la tutela continua ad essere esperibile per l'insieme dei rimedi già presenti nel c.p.i., con le modifiche apportate o in attuazione della direttiva IP Enforcement 2004/48 CE, applicabile al segreto commerciale in quanto diritto di proprietà industriale non titolato. Su questo aspetto A. OTTOLIA (nt. 23), 1129, ha rilevato connotati "differenti e innovativi" rispetto alla prassi del processo industriale, dato che, in primo luogo, queste tipologie di informazioni riservate che possono essere soggette al vincolo non attengono, generalmente, alla documentazione del processo, come per i soggetti obbligati, né, più in particolare, alle informazioni riservate, che gravano comunque sui soggetti, bensì ad una categoria più ristretta. In secondo luogo, la natura del vincolo di riservatezza assume le caratteristiche specifiche di un ordine giurisdizionale, dove la violazione ha conseguenze ulteriori e differenti rispetto alla violazione delle norme generali. Infine, il contenuto del vincolo si distingue dai generali obblighi di riservatezza che sarebbero sostanzialmente di non *facere.* Il tenore di tale disposizione induce a ritenere che gli obblighi imposti all'art. 121-*ter* c.p.i. possano arrivare a imporre specifici obblighi di *facere* destinati, ad esempio, alla predisposizione di mezzi idonei per la conservazione e la cancellazione del segreto.

commerciali, dei legittimi interessi dei terzi e del pubblico in generale con la garanzia di tutelare sempre i diritti fondamentali. In alternativa alla disposizione dell'art. 124 c.p.i. il giudice può disporre, su istanza della parte interessata, il pagamento di un indennizzo qualora la parte istante non conosceva, né avrebbe potuto conoscere, che il segreto commerciale era stato ottenuto da un terzo il quale l'aveva a sua volta acquisito in maniera illecita, o qualora le misure dell'art. 124 siano eccessivamente onerose e l'indennizzo risulti adeguato. In ogni caso è stato stabilito che l'importo dell'indennizzo non dovrà superare i diritti dovuti qualora la parte istante avesse richiesto l'autorizzazione ad utilizzare i segreti commerciali[38].

Ulteriori modifiche sono state apportate alla disciplina che regola la pubblicazione della sentenza all'art. 126 c.p.i.. Con l'art. 7 del decreto si è previsto infatti che in ogni caso debba essere garantita la riservatezza dei segreti commerciali in caso di pubblicazione della sentenza e che, nel valutare la proporzionalità, siano considerati il valore del segreto commerciale, la condotta dell'autore della violazione, l'impatto dell'utilizzazione o della rivelazione illecita di segreto commerciale ed il pericolo di ulteriori utilizzazioni o rivelazioni[39].

Con l'art. 8 del decreto vengono apportati dei cambiamenti al sistema cautelare, come stabilito all'art. 132 c.p.i., prevedendo che su istanza di parte, in alternativa all'applicazione delle misure cautelari, il giudice possa autorizzazione alla parte interessata la continuazione dell'utilizzo di segreti commerciali prestando però idonea cauzione per l'eventuale risarcimento dei danni subiti dal legittimo detentore; nel provvedere alle domande cautelari il giudice dovrà considerare le circostanze del caso, indicate all'art. 124, co. 6-*bis,* c.p.i., valutandone la proporzionalità. Infine, nel caso di perdita di efficacia delle misure cautelari,

---

[38]Come disposto dall'art. 6 d.lgs. 63/18. Si veda G. GHIDINI, G. CAVANI, (nt. 27), 39, e A. OTTOLIA (nt. 23), 1111, dove si chiarisce che l'art. 6, co. 1 del d.lgs. ha riformato l'art. 124 c.p.i. introducendo nuovi co. 6-*bis*, 6-*ter* e 6-*quarter.* Si attribuisce così al giudice la facoltà di imporre un equo indennizzo in sostituzione delle misure previste dall'art. 124 c.p.i., in particolar modo l'inibitoria della produzione e della vendita del prodotto costituite violazione del segreto commerciale. Si prevede, fra le condizioni necessarie per la degradazione di tutela, il caso che l'istante abbia ignorato incolpevolmente il fatto che "i segreti commerciali erano stati ottenuti da un terzo che li stava usando o rivelando illecitamente". La portata dell'art. 124 c.p.i. è comunque limitata alle fattispecie di acquisizione del segreto poste in essere da un soggetto in buona fede, il quale apprende solo successivamente dell'illiceità della provenienza dell'informazione, ad esempio a seguito della notificazione da parte del suo titolare.

[39] Come descritto da C. GALLI in *Il nuovo diritto del know-how e dei segreti commerciali,* Utet Giuridica, 2018, 123, la pubblicazione delle sentenza è una misura che può contribuire a rimediare alla conseguenza di un illecito, suggerendo al legislatore nazionale di novellare anche l'art. 126 c.p.i. Si è previsto però che la pubblicazione della sentenza avvenga applicando tutte le possibili misure idonee a garantire la tutela della riservatezza dei segreti commerciali. Il legislatore ha quindi introdotto due nuovi commi, 1-*bis* e 1-*ter,* che riproducono in sostanza l'art. 15 della direttiva UE. In particolar modo viene esplicitato che, per le cause in materia di *trade secrets*, è necessario che la misura della pubblicazione venga disposta solo a valle di un'attenta analisi degli interessi contrapposti delle parti, con specifico riferimento al tema della privacy, considerando inoltre gli eventuali danni alla reputazione del medesimo autore, si veda in tal senso G. GHIDINI, G. CAVANI, (nt. 27), 40.

per l'azione o l'omissione del ricorrente, quest'ultimo è tenuto al risarcimento del danno cagionato in misura adeguata[40].

Infine il decreto all'art. 9 ha previsto ulteriori modifiche al codice penale, in materia di mancata esecuzione dolosa di un provvedimento del giudice e in materia di rivelazioni di segreti scientifici o industriali, con modifiche apportate agli artt. 338, 623 del codice penale (si veda *infra* 1.4.).

1.3.1. L'articolo 98 c.p.i.

L'art. 98 c.p.i., all'interno del Capo delle norme relative all'esistenza, all'ambito e all'esercizio dei diritti di proprietà industriale, nella sezione dedicata ai segreti commerciali, apre esplicitando una definizione di segreti commerciali: sia informazioni di natura tecnico-industriale, sia informazioni di natura puramente commerciale che rispondono a determinati requisiti. Come illustrato nel co. 2 dell'art. 98 c.p.i., sono ritenuti segreti industriali anche dati relativi a prove o altri dati segreti risultanti da elaborazioni di considerevole impegno la cui presentazione è subordinata ad un'autorizzazione per l'immissione in commercio di prodotti impiegati nel settore chimico, farmaceutico o agricolo, cioè "*implicanti l'uso di nuove sostanze chimiche*".

Nell'art. 98 c.p.i. vengono disposti i requisiti necessari per l'applicazione della tutela prevista ai segreti commerciali, questi requisiti richiesti alle informazioni dell'impresa sono: lo stato di segretezza, ossia devono essere informazioni "*segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore*", le informazioni devono presentare un valore intrinseco dato il loro particolare stato di segretezza, e quindi "*abbiano valore economico in quanto segrete",* ed infine è necessaria la presenza di forme di protezione atte a mantenere inalterata la segretezza delle informazioni, perciò devono essere "*sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete*", le misure di protezione devono essere non indifferenti e adeguate al contenuto protetto, e possono consistere in misure sia fisiche che

[40] In tal senso si veda C. GALLI, (nt. 39), 132. E G. GHIDINI, G. CAVANI, (nt. 27), 40.

giuridiche (si veda *infra* capitolo 3)[41].

In linea con le disposizioni del TRIPS e della direttiva UE sui *trade secrets,* sintetizzando la trattazione dei requisiti, le informazioni devono presentare elementi essenziali di segretezza, valore economico e un'adeguata protezione, generando perciò una tipizzazione dell'istituto, che è frutto di un percorso regolamentatorio della materia; le disposizione del 98 c.p.i. riproducono in effetti una definizione dell'istituto che ricalca quella già maturata nell'ambito dei paesi anglosassoni, venendosi a delineare in Italia dapprima nel 1996 con la legge invenzioni all'art. 6-*bis,* abrogata poi nel 2005 con l'introduzione del Codice della Proprietà Industriale[42].

A questi requisiti possono correttamente rispondere il c.d. know-how tecnico, relativo a procedimenti e prodotti, frequentemente presenti in disegni tecnici, processi chimici, manuali

---

[41] Si veda l'art. 98, co. 1, c.p.i. In tal senso anche G. GHIDINI, G. CAVANI, (nt. 27), 36 e L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 510, in cui si specificano i requisiti previsti dall'art. 98 c.p.i. sul tema della segretezza. L'autore evidenzia che la nozione di segreto è relativa e non assoluta, cioè sono considerate segrete non solo le informazioni inaccessibili in generale al pubblico, ma anche quelle che non siano note o non facilmente accessibili agli operatori del settore. Non è quindi necessario che le informazioni abbiano carattere di novità assoluta, intesa propriamente come non accessibilità in qualunque luogo ed in qualunque sua forma. Il tema della relatività della tutela disposta dal legislatore determina che l'oggetto, cioè il contenuto del segreto commerciale, deve essere dimostrato, è invece esclusa qualsiasi tutela se l'informazione è conseguita in maniera indipendente o legittimamente, come disposto dal Trib. Milano 14 febbraio 2012, n. 5859, in *Giur. ann. dir. ind*., in cui si indica che: "L'art. 98 c.p.i., non dispone che le informazioni siano diversamente irraggiungibili dal concorrente: dispone che è illecita la loro sottrazione che comporta un risparmio di tempi e costi rispetto ad una loro autonoma acquisizione". Per ciò che concerne il valore economico dell'informazione, si indica che tali informazioni devono avere un valore economico in quanto soggette a vincoli di segretezza, nel senso che devono possedere una qualche utilità pratica, rendendole sfruttabili in un'attività economica d'impresa. L'utilità deve essere commisurata rispetto ad un soggetto operante nel medesimo settore, privo delle informazioni di cui si tratta nello svolgimento della sua attività d'impresa. Infine, descrivendo il terzo requisito, si puntualizza che il riferimento alla "ragionevole adeguatezza" delle misure che vengono adottate rende anche questa nozione non assoluta ma relativa. Le misure devono essere innanzitutto esigibili, si potrà dunque richiedere che vengano adottati tutti i controlli legittimamente esigibili. La valutazione di ragionevolezza andrà comunque effettuata in concreto, in base alle circostanze del caso, tenendo conto di tutti i costi delle misure in relazione alla loro efficacia. Spesso il giudice per valutare la presenza dei requisiti necessari si affida a un consulente tecnico d'ufficio (CTU), come indicato dal Trib. Milano, 14 febbraio 2012, n. 5859, in *Giur. ann. dir. ind*., in cui si specifica che l'applicazione delle disposizioni degli artt. 98 e 99 c.p.i. appare spesso supportata da CTU anche in ambito cautelare.

[42] In particolare i requisiti ricalcano la tradizione di *common law* della disciplina USA, dov'è presente un'articolata normativa, civilistica e penalistica, che tratta e tutela ampiamente i segreti commerciali, in tal senso si veda C. GARUFI, *Il brevetto europeo e i segreti commerciali,* La Tribuna, 2018, 20. A riguardo della legge invenzioni (l. inv.) nel *c.c. commentato, art. 2598. Atti di concorrenza sleale. La concorrenza sleale per scorrettezza professionale* s'indica che la rivelazione di segreti, oltre ad integrare un atto di concorrenza sleale ai sensi dell' art. 2598, n. 3, c.c, è stata successivamente disciplinata in maniera puntuale dall'art. 6-*bis* della legge invenzioni, articolo introdotto con il d.lgs. 19 marzo 1996, n. 198, che ha dato attuazione agli accordi di TRIPS del 1994. Cfr. sul punto S. SANDRI, *La nuova disciplina della proprietà industriale dopo i GATT-TRIP's*, Cedam, Padova, 1996, 135. La norma delineava una fattispecie precisa di violazione del segreto. Tuttavia, tale norma, facendo salvo il disposto dell' art. 2598, n. 3, c.c., lasciava aperta la possibilità di qualificare quale atto di concorrenza sleale per contrarietà alla correttezza professionale le ipotesi di violazione di segreto che si determinano al di fuori dell'art. 6-*bis* l. inv. Sul rapporto tra questa normativa speciale e le norme sulla concorrenza sleale, si vedano in dottrina N. ABRIANI, G. BOTTINO, *La concorrenza sleale*, a cura di N. ABRIANI, G. BOTTINO, M. RICOLFI, *Diritto industriale*, in *Tratt. Cottino*, Cedam, Padova, 2001, 311. Con l'adozione del Codice della Proprietà Industriale, il legislatore ha abrogato la l. inv. ed ha riportato, con alcune modifiche, il testo dell' art. 6-*bis* l. inv. nel c.p.i.

d'uso[43], come il know-how commerciale, che comprende dati e informazioni necessarie allo svolgimento delle funzioni commerciali di un'attività d'impresa[44], inoltre anche le informazioni relative ai clienti, elementi fondamentali e definiti come "segreti di fabbrica"[45], relativi non solo a semplici elenchi, ma anche alla loro ubicazione o relative condizioni contrattuali allegate, possono essere tutelabili come segreti commerciali. Ulteriormente a queste categorie di informazioni sono considerabili segreti commerciali anche tutte le conoscenze dell'impresa inerenti caratteristiche ed elementi di fornitori, in base alla medesima *ratio* applicata alle informazioni relative ai clienti. Infine possono rispondere ai requisiti di segretezza informazioni attinenti al know-how amministrativo, si pensi ad esempio alla documentazione necessaria per la certificazione UNI EN ISO 9001, la quale può comprendere procedure, norme, tempistiche, tecniche, sistemi di controllo qualità dell'impresa, tutte informazioni sensibili dell'impresa che possono venir correttamente tutelate, come stabilito dall'art. 98 c.p.i[46].

1.3.2. L'articolo 99 c.p.i.

In caso di mancanza di tutti o di uno dei requisiti stabili dall'art. 98 c.p.i. alle informazioni non si potrà applicare la tutela prevista per i segreti commerciali, ma sarà comunque valida la tutela fornita dal divieto di atti di concorrenza sleale, come stabilito dall'art. 2598, co. 3, c.c.: ciò è previsto dall'art. 99 c.p.i. che inizia dichiarando "*ferma la disciplina della concorrenza*

---

[43] Come indicato dal Trib. Milano, 31 marzo 2004, n. 4734, in *GADI*, rientrano in questa categoria i "disegni esecutivi degli impianti e dei procedimenti di lavorazione e produzione delle fibre", o "le modalità di attuazione di un processo industriale" come definito inoltre dall'App. Bologna, 19 maggio 1995, n. 3426, in *GADI*, o ancora "le formule chimiche segrete" come definito dall'App. Milano, 29 novembre 2002, n. 622, in *GADI*.

[44] Si veda App. Bologna, 5 giugno 1993, n. 3062, in *GADI*, che riprende quanto già indicato da Cass., 20 marzo 1991, n. 3011, in *GADI*, in cui si precisa che "hanno carattere riservato gli elenchi contenenti, oltre i nominativi di tutti i clienti e i fornitori di una società, anche l'indicazione dei volumi di affari che ciascun fornitore aveva con essa".

[45] Definizione estrapolata da Trib. Milano, 10 dicembre 1992, n. 2920, in *GADI*.

[46] Come indicato da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 20 ss. e in tal senso anche L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 509 dove si specifica che la disciplina del c.p.i. agli artt. 98 e 99 c.p.i. conferma l'applicabilità della tutela anche nel caso di sottrazioni di segreti commerciali dell'impresa diversi da conoscenze astrattamente brevettabili, come possono essere i metodi commerciali, le liste di clienti e fornitori, le tecniche finanziarie, di gestione o di marketing. Così la nuova disciplina dell'art. 98 c.p.i. non protegge soltanto le informazioni aziendali (come era previsto precedentemente per l'art. 6-*bis* l.i.) ma anche le esperienze tecnico industriali, tra le quali vanno pur sempre ricomprese quelle di natura commerciale.

sleale"[47].

Non è previsto un diritto di esclusiva assoluta per il segreto commerciale[48], ma come disposto dall'art. 99, co. 1, c.p.i., il "*legittimo detentore dei segreti commerciali di cui all'articolo 98, ha il diritto di vietare a terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare in modo abusivo*"[49]. Per modo abusivo s'intende la sottrazione di informazione in modalità illecite, ossia violando vincoli di natura legale o convenzionale, con strumenti che possono essere ritenuti illeciti, come ad esempio attraverso comportamenti volti allo spionaggio industriale.

L'art. 99, co. 1-*bis,* c.p.i., modificato dando attuazione alla direttiva UE 2016/943, stabilisce che l'acquisizione, l'utilizzazione o la rilevazione di segreti commerciali è considerata illecita se avviene anche tramite l'ottenimento di un'informazione da un terzo soggetto, il quale

---

[47] In tal senso si veda S. MAGELLI *Il know-how nell'esperienza giurisprudenziale italiana tra esclusiva e concorrenza sleale,* in *Dir. ind.*, 2016, II, 190, in cui si aggiunge che la riserva contenuta nell'art. 99 c.p.i., in ogni caso, fa salva la normativa in materia di concorrenza sleale. Si consente di ritenere sempre configurabili le fattispecie definite dall'utilizzazione di notizie riservate e di know-how dell'impresa, a condizione che tale utilizzo avvenga con modalità scorrette, danneggiando quindi il concorrente. Si veda anche la sentenza Trib. Bologna, 5 gennaio 2015, in S. MAGELLI, in cui si indica che la riserva contenuta nell'art. 99 c.p.i., che, come detto, fa salva la normativa in materia di concorrenza sleale, deve ritenersi comunque applicabile l'art. 2598, n. 3, c.c. nelle ipotesi di: "utilizzazione e divulgazione di notizie riservate o, in genere, di know-how aziendale, quando non risultino soddisfatti per intero tutti i requisiti richiesti dall'art. 98 c.p.i., costituiti appunto dalla segretezza, dal valore economico e dall'adozione di misure ragionevolmente adeguate".

[48] Come indicato da A. VANZETTI, V. DI CATALDO, *Manuale di Diritto Industriale,* Giuffrè, Milano 2018, 489 ss. Tuttavia in dottrina si riscontrano posizioni divergenti sull'estensione della tutela del segreto commerciale. Si veda, ad esempio, S. BARBARO, *Le informazioni aziendali riservate: la scelta del codice della proprietà intellettuale*, in *Diritti esclusivi e nuovi beni immateriali* a cura di G. RESTA, Utet Giuridica, Milano, 2011, 319, in cui s'indica che il tenore del testo dell'art. 99 c.p.i., nella sua formulazione previgente, suggerisce una tutela delle informazioni riservate che, prescindendo dalla concorrenza sleale prevista dall'art. 2598 c.c., può essere azionata nei confronti di chiunque avesse rivelato, acquisito e utilizzato informazioni riservate indipendentemente dall'esistenza di un rapporto concorrenziale e dalla violazione di principi di correttezza professionale e di conseguenza anche qualora ciò fosse avvenuto in buona fede. L'autore sostiene dunque che queste tipologie di informazioni riservate acquistano un vero e proprio diritto di proprietà industriale, non titolato, e come tale connotato da assolutezza, esclusività e azionabilità *erga omnes"*.

[49] Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 489 ss., G. RESTA, *Diritti esclusivi e nuovi beni immateriali,* Utet Giuridica, Milano, 2011, 290 e A. OTTOLIA, (nt. 23), 1108. Il decreto attuativo ha lasciato invariata la disposizione, dove si riconosceva al legittimo detentore il diritto di vietare a terzi di acquisire, rivelare e utilizzare in maniera abusiva le conoscenze segrete; con ciò il legislatore ha ritenuto evidentemente la normativa già conforme alla disciplina di armonizzazione europea. Tuttavia, bisogna sottolineare che, in via preliminare, mentre la condotta di violazione includerebbe, nel testo europeo, la c.d. "divulgazione" delle informazioni, la disposizione italiana disciplinata all'art. 99 si riferisce non tanto alla divulgazione ma quanto alla rivelazione, includendo nell'area dell'antigiuridicità anche tutte le condotte di cui non sia destinatario un pubblico o un gruppo, ma anche un singolo soggetto. Si realizza perciò un legittimo rafforzamento del contenuto del diritto di tutela delle informazioni. Come indicato all'art. 99 c.p.i., il diritto di vietare usi illeciti del segreto commerciale spetta al legittimo detentore, come disposto dal Trib. Bologna, sez. spec. impresa, 22 giugno 2020, n.925, in *DeJure*, in cui si specifica che: "Ai sensi dell'art. 99 c.p.i. il diritto di vietare ai terzi l'acquisto, la rivelazione o l'utilizzo dei segreti commerciali spetta al legittimo detentore dei segreti commerciali stessi. Non vi è quindi dubbio che per accedere alla tutela prevista dalla norma non occorra allegare di aver acquistato la titolarità delle informazioni riservate (a titolo originario o a titolo derivativo) e meno ancora provare la catena degli acquisti a titolo derivativo, sino al primo proprietario, essendo appunto sufficiente la legittima detenzione".

aveva a sua volta acquisito l'informazione in maniera diretta o indiretta, ma con strumenti o comportamenti illeciti. Tale situazione comporterebbe una violazione delle disposizioni dell'art. 99 c.p.i. sia nel caso che tale situazione fosse a conoscenza del nuovo acquirente, sia nel caso in cui, date le circostanze in cui tale informazione è stata acquisita, si dovrebbe conoscere o intuire la natura illecita dell'acquisizione dell'informazione a monte. L'art. 99 c.p.i. stabilisce che la violazione richiede pur sempre un comportamento abusivo e non può pregiudicare il soggetto che, in buona fede, ha recepito le competenze e le conoscenze riservate a titolo particolare per via negoziale, oppure attraverso una ricerca autonoma o processi di ingegneria inversa (c.d. *reverse engineering*)[50].

Il nuovo co. 1-*ter* dell'art. 99 c.p.i., anch'esso modificato con l'introduzione della direttiva UE 2016/943, estende la disciplina di tutela dei segreti commerciali a tutte quelle merci che vengono prodotte, offerte, commercializzate, importate, esportate o stoccate e che sono frutto di violazione in quanto beneficiano in maniera significativa di segreti commerciali acquisiti in maniera illegittima nelle fasi di progettazione, nella definizione di caratteristiche, produzione o commercializzazione[51]. L'art. 99, co. 1-*quarter,* c.p.i., prevede che i diritti e le azioni derivanti dalle condotte illecite perpetuate nell'acquisizione, nell'utilizzazione o nella rivelazione di segreti commerciali si prescrivono in cinque anni[52].

---

[50] Si veda C. GARUFI, (nt. 42), 15. e S. SERAFINI, (nt. 20), 1332 dove trattando le nuove disposizioni inerenti l'art 99 c.p.i. si sottolinea che tra le eccezioni più importanti previste dalla tutela del segreto commerciale si individua l'ottenimento in maniera autonoma del contenuto coperto da segreto, ossia attraverso attività di *reverse engineering*, oppure attività di decodificazione delle informazioni, attività che permettono la riproduzione del prodotto contenente il segreto a partire dall'analisi della sua struttura e del suo funzionamento. Si ritiene però il *reverse engineering* un'attività lecita soltanto se non è eccessivamente difficoltosa per gli esperti del settore.

[51] In tal senso si veda G. GHIDINI, G. CAVANI, (nt. 27), 38 e A. OTTOLIA (nt. 23), 1110. Si precisa che il nuovo co. 1-*ter* dell'art. 99 c.p.i. è intervenuto in materia di commercializzazione di beni contenenti un segreto commerciale, si è dunque previsto un diritto di sequela che qualifica l'utilizzo illecito di informazioni segrete ad una serie di attività di vendita di prodotti e merci e commercializzazione che incorporano il contenuto di un segreto o ne costituiscano una funzionale derivazione, eseguito con la consapevolezza o la colpevole inconsapevolezza dell'origine illecita dell'informazioni. Queste condotte illecite si riferiscono a soli soggetti che non partecipano alla fabbricazione diretta ma che sono meri aventi causa di coloro che hanno acquisito o utilizzato illecitamente il segreto. Questa ipotesi di illecito diretto sono suscettibili di tutela inibitoria, determinando una sostanziale estensione dell'oggetto del diritto alla tutela. Si pensi, ad esempio, al caso di un nuovo datore di lavoro, che consapevolmente utilizza informazioni illecitamente sottratte da un suo dipendente all'ex datore di lavoro.

[52] Come indicato da G. GHIDINI, G. CAVANI, (nt. 27), 38 e A. OTTOLIA (nt. 23), 1113. Si sottolinea che la norma sulla prescrizione non aveva antecedenti nella disciplina europea dei diritti di proprietà industriale e intellettuale. La disposizione di una prescrizione quinquennale è stata prevista per tutelare la certezza del diritto, che da sempre giustifica l'esistenza dell'istituto della prescrizione ed il processo di inarrestabile frammentazione che ne ha caratterizzato l'evoluzione. Particolare rilievo assumono dunque gli interessi delle PMI per questa materia. La prescrizione quinquennale si applica inoltre perfettamente alle ipotesi di illecito acquiliano, il legislatore si è così adeguato alla durata massima della prescrizione prevista della direttiva UE 2016/943 che è stabilita per un massimo di sei anni.

1.3.3. L'articolo 2598, co. 3, c.c.

Alla luce della recente giurisprudenza e dalla dottrina, come stabilito dall'art. 99, co. 1, c.p.i., dove si prevede "*ferma la disciplina della concorrenza sleale*", si è riconosciuto che una tutela sussidiaria contro la violazione di un segreto commerciale è presente al n.3 dell'art. 2598 del Codice Civile (da ora c.c.), affrontando la disciplina perciò come una fattispecie tipica di concorrenza sleale che, seppur non esplicitamente disciplinata, rientra tra quelle che vengono costituite come una "clausola generale"[53]. All'art. 2598, n.3, c.c. sono definiti, come concorrenza sleale, tutti gli atti non conformi alla correttezza professionale ed idonei a danneggiare l'altrui impresa. Questi atti si possono classificare in due diversi gruppi: atti di concorrenza sleale che alterano la situazione del mercato, senza riferimento ad un particolare imprenditore, ed atti che invece sono tipicamente rivolti contro un determinato concorrente.

La sottrazione di segreti commerciali può rientrare nella seconda fattispecie di atti e può essere legata ad ulteriori atti di concorrenza sleale, qual è lo storno di dipendenti da un'impresa. Questa situazione può comportare ad un datore di lavoro serie minacce, quali ad esempio la rivelazione di notizie destinate a rimanere riservate a diretti concorrenti da parte di dipendenti infedeli o ex dipendenti che fungono da "talpe"[54] o, in casi più estremi, in attività di vero e proprio spionaggio industriale. E' infatti tutt'altro che infrequente nella pratica situazioni che vedono l'ex dipendente compiere comportamenti volti a sottrarre informazioni o documenti di natura tecnica o commerciale al proprio precedente datore di lavoro, mettendoli poi a disposizione ad un altro soggetto concorrente con il quale ha avviato una

---

[53] Si veda A. VANZETTI, V. DI CATALDO, (nt. 33), 99 ss. In tal senso si veda la sentenza del Trib. Bologna, 27 luglio 2015, n. 2340 in *Giurisprudenzadelleimprese.it*, in cui oggetto del segreto commerciale erano "disegni tecnici ed elaborati progettuali, costruttivi e meccanici, per un attacco da scialpinismo". S. MAGELLI, (nt. 47), 194, indica che l'appropriazione di informazioni tecnico-aziendali riservate, anche se non protette come previsto dall'art. 98 c.p.i., costituiscono comportamento illecito contrario alla correttezza professionale e, quindi, concorrenza sleale ai sensi dell'art. 2598, n. 3, c.c. come definito anche dal Trib. Bologna, 5 gennaio 2015, indirettamente anche Trib. Milano, 12 novembre 2014, n. 13320, in S. MAGELLI, (nt. 47), 194 e Trib. Milano, 21 febbraio 2011, n. 5695, in *Giur. ann. dir. ind*. Si veda anche G. GHIDINI, G. CAVANI, (nt. 27), 37.

[54] A tal proposito si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 115 ss. e il commento alla sentenza Cass, sez. I, 31 marzo 2016, n. 6274 in A. GERACI, *Storno di dipendenti: illecito se attuato per utilizzare il know-how del concorrente, in Dir. ind.* 2017, IV, 324, in cui la Cassazione ha ricordato che: "Nello storno di dipendenti l'intento di nuocere l'impresa antagonista può ravvisarsi ogni qualvolta tale condotta sia stata attuata al fine di appropriarsi dei frutti dell'attività del concorrente". Lo storno di dipendenti è un atto di concorrenza sleale nei casi in cui consenta, a chi lo pone in essere, di attingere e acquisire in maniera illecita il know-how del concorrente, inteso come "il patrimonio di conoscenze e di contatti per lo sviluppo dell'attività". Per le stesse ragioni è considerato ad esempio illecito concorrenziale la condotta consistente nell'appropriazione dei tabulati recanti i nominativi telefonici dei clienti e dei distributori dell'impresa concorrente. Si veda anche P. DI TULLIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 8), 2110, l'orientamento giurisdizionale è oramai consolidato a ritenere la sottrazione dei segreti commerciali di un imprenditore concorrente atti di concorrenza sleale, tramite attività volte allo spionaggio industriale o attraverso un dipendente infedele.

nuova collaborazione. L'ex dipendente sarà perseguibile penalmente, anche solo per l'indebita appropriazione, ovvero per il furto di materiale segreto, trattando il caso specifico del 623 c.p. (si veda *infra* 1.4). L'impresa che riceve dall'ex dipendente "talpa" documenti segreti, acquisiti a sua volta tramite comportamenti illeciti, anche laddove questi documenti non presentino i requisiti del 98 c.p.i., potranno e dovranno essere perseguibili per la commissione di atti di concorrenza sleale[55].

La tutela offerta dall'art. 2598, n.3, c.c., è volta ad assicurare all'imprenditore il vantaggio competitivo che deriva dall'utilizzazione economica delle informazioni segrete, vietando comportamenti scorretti diretti ad un utilizzo illecito dei frutti dell'altrui lavoro e che possono bensì rientrare in atti di concorrenza parassitaria. In questa disciplina le informazioni dell'impresa, pur non presentando una vera e propria tutela specifica, sono oggetto di una tutela indiretta, dato che saranno considerate illecite tutti gli atti di terzi volti all'appropriazione delle informazioni segrete con modalità contrarie alla correttezza professionale. La tutela dei segreti non sarà dunque legata a rigidi criteri che ne definiscono l'esatta estensione della tutela, ma verrà effettuata una valutazione caso per caso per determinarne l'applicazione, in base alla portata normativa considerata dalla clausola della correttezza professionale[56]

Ci si pone ora il quesito se possa ritenersi lecito l'utilizzo d'informazioni guadagnate dall'ex dipendente nel corso della sua attività lavorativa e che successivamente vengono sfruttate in altre realtà aziendali. In questo caso la necessità di tutelare il segreto si contrappone con il principio secondo cui l'ex dipendente e il nuovo datore di lavoro possono utilizzare in maniera legittima esperienze e conoscenze tecniche e di mercato acquisite dal dipendente nell'esercizio delle sue mansioni, anche presso l'ex datore di lavoro. La giurisprudenza afferma infatti che si tratta di *"aspetti di particolare delicatezza, incidendo su posizioni costituzionalmente garantite attinenti, da un lato, alla libertà di iniziativa economica e, dall'altro, alla libera espressione della personalità: principi che possono porsi in virtuale conflitto, quando l'espressione di capacità personali di un soggetto costituiscano eventuale*

---

[55] Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 34 ss. inoltre A. GERACI, (nt. 54), 5, nel commentare la sentenza Cass., sez. I, 31 marzo 2016, n. 6274, si precisa che il legislatore considera illeciti atti che pur di per sé leciti, in concreto, sono invece attuati in violazione delle regole di correttezza e siano, al contempo, idonei a danneggiare l'altrui impresa.

[56] Come indicato da G. RESTA, (nt. 48), 290.

pregiudizio per l'evolversi di un impresa"[57]. Per superare l'*impasse* la giurisprudenza ha definito che le informazioni, per dar luogo ad un illecito, devono presentare una forte caratterizzazione di segreto o essere specifiche conoscenze attinenti all'ambito di attività svolta in via riservata dall'impresa. La Suprema Corte di Cassazione ha stabilito che *"le capacità professionali che il dipendente abbia acquisito o migliorato nel corso del pregresso rapporto di lavoro costituiscono un suo uso esclusivo patrimonio professionale liberamente utilizzabile, mentre le conoscenze specifiche attinenti all'ambito riservato dell'altrui impresa permangono riservate e inutilizzabili in virtù delle regole di correttezza"*[58]. In tal senso, il divieto di utilizzo delle informazioni segrete acquisite nel precedente rapporto di lavoro si rivolgerebbe sia nei confronti dell'ex dipendente, vietando possibili atti volti a sviare a proprio vantaggio le conoscenze e le informazioni segrete dell'impresa di provenienza, quanto nei confronti del datore di lavoro, necessitando l'istituzione di vincoli volti ad evitare posizioni di rendita parassitaria[59].

Tra la disciplina dell'art. 2598, n.3, c.c. e gli artt. 98 e 99 c.p.i. si può quindi ipotizzare la presenza di un sistema cumulativo di protezione dei segreti commerciali, ciò, come già

---

[57] Come disposto dalla Cass., 20 marzo 1991, n 3011; così anche Cass., 11 ottobre 2002, n. 14479 G. GHIDINI, G. CAVANI, (nt. 27)

[58] Si veda in tal senso la sentenza della Cass. 20 marzo 1991, n. 3011 in G. GHIDINI, G. CAVANI, (nt. 27), 142 e P. DI TULLIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 2110. Trattando la nozione di segreto qui esposta, si ritiene che tale comprende segreti industriali e commerciali o notizie che l'imprenditore non ritenga di mettere a disposizione del pubblico. Così, ad esempio, dovranno ritenersi segrete le liste clienti, nel caso non siano agevolmente accessibili, specialmente se indicanti informazioni di natura commerciale. Deve comunque trattarsi di notizie che rivestano un oggettiva rilevanza, contenendo certi dati tecnici o commerciali, oggettivamente idonee a restare sconosciute a terzi soggetti. E' invece irrilevante se si siano notizie relative a trovati non brevettabili, oppure semplici conoscenze richieste per produrre un bene, o ancora per attuare un processo produttivo, anche per un corretto impiego di una certa tecnologia. Sono state ritenute segrete tutte le conoscenze dell'impresa che non appartengono allo stato della tecnica. La necessità della segretezza esclude l'illecito quando le notizie sono ottenute in altro modo, in particolar modo attraverso l'esame, pur analitico o scompositivo, del prodotto, tramite *reverse engineering*. Come stabilito da S. MAGELLI, (nt. 47), 194 perciò, sintetizzano, atti di concorrenza sleale si possono rilevare in caso di: rapidità della progettazione, sostanziale identità del progetto, mancata prova del campione per un *reverse engineering,* oppure l'assunzione di un ex dipendente. Tutti questi elementi possono costituire indizi gravi, precisi e concordanti, che riscontrano la contrarietà alla correttezza professionale, come stabilito dall'art. 2598 c.c., con il presupposto sottostante del rapporto di concorrenza.

[59] In tal senso la Cass., 11 ottobre 2002, n.14479, in G. GHIDINI, G. CAVANI, (nt. 27), 142 ha affermato che: "In materia di concorrenza, nel momento in cui l'ex dipendente utilizzi la professionalità acquisita alle dipendenze di un altro imprenditore si rendono applicabili le regole della concorrenza professionale, che rinviano al buon costume commerciale, la cui linea di confine può individuarsi nel divieto della concorrenza parassitaria, volta a sviare a proprio vantaggio i valori aziendali di imprese preesistenti, e in particolare di quelle di provenienza. Al riguardo non può tuttavia considerarsi illecita l'utilizzazione del valore aziendale esclusivamente costituito dalle capacità professionali dello stesso ex dipendente, non distinguibili dalla sua ex persona; poiché, in caso contrario, si priverebbe al risultato, duplicemente accettabile, di vanificare i valori della libertà individuale inerenti alla personalità del lavoratore, costringendolo ad una situazione di dipendenza che andrebbe oltre i limiti contrattuali, e di privilegiare nell'impresa, precedente datrice di lavoro, una rendita parassitaria derivante, una volta per tutte, dalla scelta felicemente a suo tempo fatta con l'assunzione di quel dipendente". Si veda anche G. RESTA, (nt. 48), 305 ss.

indicato inizialmente, può essere confermato dal richiamo nell'art. 99 del c.p.i. alla concorrenza sleale.

La differenza sostanziale tra le due discipline riguarda da un lato i possibili soggetti coinvolti, la regolamentazione degli articoli del c.p.i. sono infatti rivolti ad una generalità di consociati, a prescindere dell'esistenza tra le parti di un rapporto di natura concorrenziale. Altra differenza è rilevata nell'individuazione del "tipo" di informazione da tutelare e delle "modalità" di acquisizione illecita di segreto commerciale. Nell'art. 2598, n.3, c.c., la determinazione di segreto commerciale si presenta in una forma più "soft" e meno vincolante rispetto i requisiti richiesti per l'identificazione di un'informazione tutelabile come segreto commerciale del 98 c.p.i., ampliando quindi le possibili applicazioni della tutela. La Suprema Corte ha infatti stabilito che le notizie e le informazioni aziendali ritenute tutelabili dal n.3 art. 2598 c.c. come sottrazione di segreto commerciale e contrarie ai principi di concorrenza leale, possono venir applicabili nel caso in cui "*pur senza essere dei veri e propri segreti, l'impresa concorrente non abbia messo, né ritenga di mettere, a disposizione del pubblico*". Quindi, diversamente da quanto previsto dall'art. 98 c.p.i., è sufficiente un interesse da parte del titolare di mantenere certe informazioni segrete per ritenerle tali, senza una valutazione effettiva di quello che è il valore economico e delle misure attuate per mantenere tali informazioni non disponibili al pubblico; la tutela codicistica sarà dunque invocabile in casi nei quali non ricorrano tutti i requisiti previsti dal 98 c.p.i., ma tuttavia la loro acquisizione sia avvenuta con modalità scorrette[60].

L'art. 2598, n.3, c.c. offre quindi una tutela che possiamo definire come sussidiaria, infatti qualora notizie meno qualificate in termini di segretezza venissero sottratte in maniera contraria alla correttezza professionale, si potrà certamente configurare un illecito art. 2598, n. 3, c.c., tant'è che i giudici, in caso di violazione di segreti, fanno più spesso ricorso a questa disciplina. In questi casi, peraltro, va esclusa la competenza delle sezioni specializzate in

---

[60] Si veda G. GHIDINI, G. CAVANI, (nt. 27), 37, A. VANZETTI, V. DI CATALDO, (nt. 48), 117 ss. e L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 510. Riferendosi all'art. 99 c.p.i., l'autore precisa che l'art. 2598 n.3 c.c. resta ragionevolmente applicabile a tutti gli atti di acquisto, utilizzazione e divulgazione di segreti commerciali d'impresa, per i quali non siano soddisfatte le condizioni stabilite dall'art. 98 c.p.i., ma sussistano parimenti, i requisiti soggettivi ed oggettivi prescritti per l'azione della concorrenza sleale. Così, ad esempio, la sottrazione con mezzi o modalità illecite di dati oggettivamente riservati, per i quali non fossero applicate le misure di segretezza adeguate ed esigibili dall'art. 98 c.p.i. Si pensi ulteriormente, ad esempio, al caso in cui le conoscenze tecniche dell'impresa, anche se facilmente desumibili o determinabili dall'analisi del prodotto dell'impresa concorrente, e dunque non propriamente segrete, sono state acquisite da una terza impresa attraverso la sottrazione di disegni di proprietà dell'impresa concorrente. Ciò consentirebbe di risparmiare costi e tempi, che sarebbero invece necessari per effettuare attività di *reverse engineering* dell'altrui prodotto, conseguendo un vantaggio concorrenziale che risulta di per sé illegittimo.

materia d'impresa, mentre è affermata quella della sezione ordinaria competente per le fattispecie di concorrenza sleale c.d. pura[61].

1.4. La tutela penale dei segreti commerciali

Con gli artt. 622 e 623 del Codice Penale (da ora c.p.) il legislatore ha posto le basi per la tutela penale del segreto commerciale con lo scopo di proteggere il know-how, le attività e gli investimenti aziendali da comportamenti che prevedano una rivelazione o l'impiego di segreti di tipo scientifico o industriale[62].

Mentre l'art. 622 c.p. prevede una reclusione fino a un anno o una multa da euro 30 a euro 516 in caso di rivelazione e impiego di conoscenze e know-how commerciale in violazione di un segreto professionale, l'art. 623 c.p. stabilisce che chiunque, per il proprio stato o per la propria professione, rivela o impiega segreti commerciali, è punito con la reclusione fino a due anni; la tutela dell'art. 623 c.p. sembra essere più generica e adeguata ad un confronto con la disciplina che abbiamo illustrato degli artt. 98 e 99 c.p.i[63].

---

[61] Si veda G. RESTA, (nt. 48), 293 e G. GHIDINI, G. CAVANI, (nt. 27), 38. Un esempio di applicazione del 2598 c.c. è la già citata sentenza del Trib. Bologna, 27 luglio 2015 n. 2340, dove si specifica che: "Non vi è prova che la società attrice avesse predisposto dispositivi o presidii volti ad impedire l'accesso e la conoscenza dei dati tecnici riportati nei suddetti disegni, né che avesse quantomeno impartito specifiche direttive in tal senso [..] insufficiente a conferire ai dati aziendali in esame il carattere della segretezza nell'accezione di cui alla lett. c) dell'art. 98 c.p.i." ma trattandosi di "informazioni riservate, nel senso, sopra delineato, di non facile accessibilità al loro contenuto costituiscono dunque, condotta di concorrenza sleale per violazione dei principi della correttezza professionale la condotta, potenzialmente dannosa, volta a carpire notizie riservate, anche non costituenti segreto industriale, relative ai processi produttivi e alle sostanze utilizzate per realizzare un dato prodotto da parte di un'impresa concorrente, senza necessità di accertare la presenza di prodotti simili sul mercato. Conseguentemente, deve ritenersi violato il regime di leale concorrenza, a norma dell'art. 2598, n. 3, c.c.". Commentando tale sentenza S. MAGELLI, (nt. 47), 194, la definisce come "significativa" per la trattazione della materia, in quanto in questa sentenza il Tribunale ha riscontrato la sussistenza del requisito della riservatezza. Si evidenzia inoltre che il requisito della rilevanza economica, è legato, da un lato, al significativo grado di penetrazione del mercato raggiunto dai prodotti ad oggetto del processo e, dall'altro, dall'indubbio ed evidente vantaggio concorrenziale acquisito dalla società convenuta in pochi mesi, in un segmento di mercato che sarebbe ad essa assolutamente inedito. Il Tribunale non ha tuttavia accolto la domanda della società attrice per l'applicazione delle disposizioni dell'art. 98 c.p.i., in quanto non ha ritenuto ravvisabile, o comunque non sufficientemente dimostrata, la sussistenza dell'ulteriore terzo requisito disposto dal suddetto articolo, affermando che la società attrice non ha dato prova di aver predisposto dispositivi o misure volte ad impedire l'accesso o la conoscenza dei dati tecnici riportati nei suddetti disegni, né aveva impartito specifiche disposizioni, adeguando misure di protezione. Il Tribunale ha dunque affermato che non era sufficiente aver custodito le informazioni in un personal computer privato, dotato di password, ed in uso esclusivo al coprogettista. Come visto in questo paragrafo però, la non configurabilità della dedotta responsabilità per l'illecito non ha precluso alla giurisdizione di riscontrare la violazione del regime di concorrenza sleale all'art. 2598, n. 3, c.c. per sottrazione di dati riservati, applicando dunque tale disciplina in maniera sussidiaria.

[62] In tal senso si veda G. GUALTIERI, *La tutela penale del know how: la violazione del segreto industriale,* in *Dir. ind.*, 2018, II, 161. Si specifica che nell'ambito dell'ordinamento italiano, la tutela penale del know-how è individuato agli artt. 622 e 623 c.p., i quali rispettivamente sanzionano la rivelazione o l'impiego di segreti professionali ovvero di segreti scientifici o commerciali. Il delitto di rivelazione di segreti scientifici e commerciali sarebbe collocato nell'ambito dei delitti contro l'inviolabilità dei segreti.

[63] In tal senso si esprime anche A. CRESPI, *La tutela penale del segreto*, Priulla, Palermo, 1952, 192.

Si tratta innanzitutto di rivelazioni di segreti scientifici e industriali collocati nell'ambito di delitti contro l'inviolabilità dei segreti, dove il bene tutelato è analogo a quello previsto all'art. 622 c.p. e dagli artt. 98 e 99 c.p.i.[64], al contempo, però, presentare alcune differenze: l'art. 623 c.p. afferma che la tutela si applica "*per segreti commerciali o di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche*"[65], senza quindi nessun riferimento a forme particolari di misure adottate per mantenere la segretezza, differentemente da quanto stabilito all'art. 98 del c.p.i., dove invece si fa riferimento a informazioni "*sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete*" e, in aggiunta, senza una valutazione di un presunto valore economico del segreto, come invece stabilito sempre all'art. 98 c.p.i., tutte queste disposizioni non trovano dunque alcun riscontro nel dettato della norma penale[66].

Il know-how nella disciplina penale per essere tutelabile come segreto commerciale dev'essere fonte di un vantaggio competitivo che assicura un suo possesso esclusivo sul piano commerciale e l'illecito deve rientrare tra i delitti contro la libertà individuale costituendo la base della vita imprenditoriale sul piano della concorrenza[67]. Il know-how tutelabile come segreto commerciale negli artt. 622 e 623 c.p. è inteso come patrimonio cognitivo e

---

[64] Come espresso da G. GUALTIERI, (nt. 62), 164, dove si indica che le nozioni di invenzioni e scoperte industriali, richiamate dalla normativa penale, riguardano informazioni di natura tecnica industriale, sostanzialmente analoga rispetto a quelle definita all'art. 98 c.p.i. La giurisprudenza ha ritenuto la presenza di una violazione del segreto professionale nei casi di "condotta di chi, nell'ambito di un contratto di franchising, riveli a terzi i dati relativi ai prezzi praticati e alla percentuale di ricarico operata nei confronti delle società affiliate" come indicato dalla Cass. pen., sez. V, 15 marzo 2017, n. 17806 in G. GUALTIERI, (nt. 62), o "nella rivelazione di informazioni inerenti codici dei prodotti, prezzi di vendita, clientele, quantità vendute, provvigioni, costi" come disposto dalla Cass. pen, sez. V, 7 marzo 2016, n. 34913 in G. GUALTIERI, (nt. 62), "nella rivelazione di specifiche politiche commerciali", come indicato dalla Cass. pen., sez. V, 16 febbraio 2016, n. 29205, in G. GUALTIERI, (nt. 62), "nella abusiva duplicazione informatica e nel successivo impiego di "dati relativi ad una società cliente", come disposto dalla Cass. pen., sez. V, 28 ottobre 2014, n. 17756 in G. GUALTIERI, (nt. 62) e "nella rivelazione di "dati e offerte commerciali" come indicato dalla Cass. pen., sez. V, 26 ottobre 2010, n. 44840 in G. GUALTIERI, (nt. 62).

[65] In tal senso si veda G. GUALTIERI, (nt. 62), 162, in cui si illustra il requisito della segretezza, indicando che nonostante l'apparente ambiguità della locuzione delle notizie destinate a rimanere segrete, l'applicazione dell'art. 623 c.p. presuppone, per chiara necessità, l'esistenza di una situazione di segretezza, che si intende appunto far durare nel tempo. Perciò deve rilevarsi la volontà del titolare a mantenere il segreto inalterato, in maniera espressa o tacita, dove l'oggetto dell'informazioni deve riguardare elementi che non siano già notorie al pubblico.

[66] Si veda S. GIAVAZZI, *La tutela penale del segreto industriale*, Giuffrè, Milano, 2012, 508. e A. OTTOLIA, (nt. 23), 1133. L'autore sottolinea come sul piano dell'oggetto materiale, su cui ricade tale condotta, non vengano specificati nel testo dell'art. 623 c.p. i requisiti di tutela, che sono invece previsti nell'art. 98 c.p.i.

[67] Come affermato da S. GIAVAZZI, (nt. 66), 508, questi delitti andrebbero contro la libertà individuale e la tutela dell'esercizio di attività industriale e imprenditoriale, questo nei riguardi di quelle informazioni tecniche che costituiscono la base vitale dell'attività imprenditoriale. Sul piano della concorrenza, tale conoscenza può infatti rafforzare la posizione di alcune imprese che svolgono un'attività nello stesso campo o nello stesso mercato, determinandone l'acquisizione di vantaggi competitivi che altrimenti non sarebbero a loro disposizione.

organizzativo, necessario per la costruzione, l'esercizio e la manutenzione di un apparato industriale, riferendosi ad un intero patrimonio di conoscenze di un'impresa, frutto di esperienze, ricerca e investimenti accumulati negli anni, proponendo perciò una lettura più estensiva rispetto alla disciplina civilistica, assicurando una tutela più incisiva[68].

Si può quindi affermare che la protezione di un segreto commerciale può essere prevista sia ai sensi dell'artt. 98 e 99 c.p.i. ma anche attraverso un'ulteriore integrazione della disciplina penale disposta dall'art. 623[69]. Il titolare di un segreto commerciale, soggetto che vede i suoi diritti su tali informazioni violati, può perciò promuovere sia un'azione civile per un risarcimento dei danni come stabilito dagli artt. 98 e 99 c.p.i. ma anche un'azione penale, in modo tale da richiedere una condanna per il responsabile. Si evidenziano però, tra le due discipline, ulteriori differenze per ciò che concerne il regime dell'onere della prova e le possibili parti coinvolte. Nell'azione penale, infatti, il convenuto dovrà dimostrare la rivelazione e/o l'impiego del segreto, per un proprio o altrui profitto, da parte della persona che ne era venuta a conoscenza dello stesso in ragione dei propri doveri di ufficio procedendo, necessariamente ai sensi dell'art. 27 della Costituzione, sia nei confronti di chi detiene il segreto, che verso chi detiene la posizione di garanzia all'interno dell'impresa, soggetto che sfrutta a proprio vantaggio la propria particolare posizione per divulgare il segreto. Diversamente nell'azione civile si dovrà dimostrare necessariamente l'esistenza di tutti i

---

[68] Tale principio è stato affermato dalla Cass. pen,, 11 febbraio 2020, n. 16975, in *Giurisprudenzadelleimprese.it* in cui s'indica che: "La dottrina e la giurisprudenza concordano nel ritenere che la copertura offerta dall'art. 623 c.p. vada oltre quella predisposta dall'ordinamento civilistico all'invenzione brevettabile, ed infatti il giudice di legittimità ha più volte affermato che, ai fini della tutela penale del segreto industriale, novità (intrinseca od estrinseca) ed originalità non sono requisiti essenziali delle applicazioni industriali, poiché non espressamente richiesti dal disposto legislativo e perché l'interesse alla tutela penale della riservatezza non deve necessariamente desumersi da tali caratteristiche delle notizie protette. Questo vuol dire che, anche se la sequenza di informazioni, che, nel loro insieme, costituiscono un tutt'uno per la concretizzazione di una fase economica specifica dell'attività dell'azienda, è costituita da singole informazioni di per sé note, ove detta sequenza sia invece non conosciuta e sia considerata segreta in modo fattivo dall'azienda, essa è di per sé degna di protezione e tutela. Non è necessario, cioè, che ogni singolo dato cognitivo che compone la sequenza sia "non conosciuto"; è necessario, invece, che il loro insieme organico sia frutto di un'elaborazione dell'azienda. E' attraverso questo processo, infatti, che l'informazione finale acquisisce un valore economico aggiuntivo rispetto ai singoli elementi che compongono la sequenza cognitiva. E' ciò che accade, appunto, nel caso di una azienda che adotti una complessa strategia per lanciare un prodotto sul mercato: i suoi singoli elementi sono senz'altro noti agli operatori del settore, ma l'insieme può essere stato ideato in modo tale da rappresentare un qualcosa di nuovo e originale, costituendo, in tal modo, un vero e proprio tesoro dal punto di vista concorrenziale per l'ideatore".

[69] Come sostenuto anche A. OTTOLIA, (nt.23), 1132; la norma all'art. 623 c.p era stata intesa, secondo l'autore e una parte rilevante della dottrina, ma anche di alcune posizioni giurisprudenziali, nel senso di presupporre una corrispondenza tra quella che è la fattispecie penale e quella civile. Si è così riconosciuto nella norma disciplinata del c.p.i. elementi integrativi alla normativa penalistica. Si valorizza così una lettura in senso sistematico delle due norme, evitando una tutela penale più estesa di quella civile.

requisiti stabiliti dall'art. 98 c.p.i., con l'ulteriore possibilità di valutare se procedere nei confronti della persona fisica che rivela il segreto o dell'impresa che se ne avvantaggia.

Il d.lgs 11 maggio 2018, n. 63 ha modificato notevolmente la disciplina del 623 c.p., apportando dei cambiamenti indirizzati a procedere con una maggiore tutela in particolare in materia digitale: si è infatti disposta una sanzione più rilevante per quei reati di sottrazione di segreti commerciali commessi attraverso l'utilizzo di strumenti informatici. L'art. 623 c.p. infatti cita che "*se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata*". Ciò dimostra la sempre maggiore attenzione del legislatore nella protezione di segreti commerciali in formato digitale, in quanto sempre più spesso tali informazioni sono soggette a violazioni tramite l'utilizzo di strumenti informatici.

Tuttavia bisogna evidenziare che le norme penali non hanno avuto grande riscontro a livello applicativo, in particolare dagli anni settanta è prevalsa un'interpretazione restrittiva degli artt. 622 e 623 c.p., configurando un'azione penale solo nei confronti di ben individuate categorie di soggetti che utilizzano e rivelano notizie destinate a rimanere segrete, quali informazioni scientifiche o applicazioni industriali, di cui si è venuti a conoscenza in un ambito lavorativo. Non si tratta quindi di una tutela *erga omnes,* bensì applicabile in certi *status,* in particolare in relazione all'inquadramento lavorativo in cui avviene illecito. In questi termini l'utilizzo della tutela penale si pone in un rapporto di complementarietà con la disciplina dell'art. 2105 c.c. inerente l'obbligo di fedeltà e la correttezza professionale in un rapporto tra dipendente e datore di lavoro[70].

1.5. Riflessi in bilancio

Sia nella disciplina civilistica che nella disciplina penale si è trattato di segreto commerciale come di informazioni a disposizione dell'impresa, queste informazioni possono avere diversa natura o carattere, possono appunto essere inerenti all'ambito tecnico-industriale, oppure commerciale o scientifico. Se si volesse però sintetizzare queste diverse tipologie di

[70] Così la Cass. pen., 18 maggio 2001, n. 25008, in G. RESTA, (nt. 44), 288 ss, che individua il bene protetto dall'articolo 623 c.p. nella libertà dell'attività scientifica, tecnica e inventiva, e il conseguente diritto alla riservatezza dell'attività stessa, cui corrisponde il dovere di terzi a non violarla. Si veda anche G. RESTA, (nt. 44), 288 ss. Concludendo G. GUALTIERI, (nt. 62), 167, evidenzia che la tutela penale del know-how ha senz'altro avuto un carattere molto residuale. Questo non sarebbe dovuto dai limiti posti alla norma penale ma anzi, gli artt. 622 e 623 c.p., secondo l'autore, sono senz'altro idonei a coprire tutte le forme di know-how segreto normalmente riconosciuto. Il problema sarebbe invece più pratico e deriverebbe dall'entità delle sanzioni, ma soprattutto, dalla previsione della perseguibilità a querela di parte, che senza dubbio giustifica la ritrosia da parte della magistratura a svolgere indagini, spesso complesse e dispendiose, che rischiano concretamente di venir vanificate da accordi fra le parti coinvolte.

informazioni in un'unica e ampia definizione le si potrebbe definire come il know-how dell'impresa[71].

Il know-how è l'insieme di saperi e abilità, competenze ed esperienze necessarie per svolgere determinate attività all'interno di settori industriali e commerciali[72], applicabili in campi molto variegati. Solo per citarne alcuni, possiamo considerare il know-how come l'insieme delle regole istituite all'interno dell'organizzazione dell'impresa, le conoscenze impiegate nella commercializzazione di prodotti, le tecniche di vendita e, più in generale, le informazioni inerenti la gestione di un'attività produttiva. Quest'espressione è ormai utilizzata da qualche decennio nella prassi del diritto industriale e commerciale a livello internazionale ed ha trovato anche ormai piena applicazione nella cittadinanza giuridica del nostro ordinamento grazie all'intervento del legislatore comunitario[73].

Sebbene nel codice civile non sia presente una chiara esplicitazione del temine know-how, si può trovare invece una precisa definizione all'interno del regolamento CE 772/04, dove nelle premesse viene indicato come know-how "*un patrimonio di conoscenze pratiche non brevettate, derivante da esperienze e da prove, patrimonio che è (i) segreto, vale a dire non generalmente né facilmente accessibile; (ii) sostanziale, vale a dire significativo e utile per la produzione dei prodotti contrattuali; e (iii) individuato, vale a dire descritto in modo sufficientemente esauriente, tale da consentire, di verificare se risponde ai criteri di segretezza e sostanzialità*".

Abbiamo già elencato alcune possibili tipologie di documenti tutelabili come segreti commerciali, questi documenti possono riportare al loro interno informazioni inerenti il know-how dell'impresa; per le imprese è sempre più necessario conservare correttamente

---

[71] Conferma in tal senso proviene dalla Circolare 7 aprile 2016, n. 11/E dell'Agenzia delle Entrate (di cui all'art. 1, lettera i, del Regolamento CE 27.4.2004, n. 772/2004) in cui viene definito il know-how come "le informazioni aziendali ed esperienze tecnico-industriali giuridicamente tutelabili". In questa categoria di informazioni aziendali ed esperienze tecnico-industriali sono comprese quelle commerciali o scientifiche, proteggibili come informazioni segrete il cui legittimo detentore è titolare di un diritto di proprietà industriale, come disposto agli artt. 98 e 99 c.p.i.

[72] Si veda L. RAMACIOTTI, *Know how,* in Treccani, Dizionario di Economia e Finanza, 2012. Come presentato anche da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 8, la traduzione letteraria di know-how è "di saper (come) fare" ma è pressoché inutilizzata, per lo meno negli ambienti giuridici.

[73] Come spiegato da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 8, la giurisprudenza ha da sempre colto la dizione di prassi del termine know-how anche in maniera indipendente, prescindendo da una sua esatta definizione giuridica e fianco tautologicamente. In tal senso si veda la sentenza Trib. Bologna, 5 giugno 1993, in *GADI,* 3062, dove si indica che le informazioni dell'impresa inerenti le imprese fornitrici e i materiali utilizzati dai concorrenti costituivano appunto "know-how" della società. Ancora A. QUAGLI in *Bilancio e principi contabili 2020,* Ipsoa, 2020, 97, definisce il know-how come: "Conoscenze idonee alla brevettabilità ma di fatto non brevettate o, comunque, non note o facilmente accessibile agli esperti".

questi supporti materiali in quanto tali rappresentano requisiti ontologici e non elementi ulteriori o accessori rispetto alla verifica della sussistenza del diritto alla tutela del loro know-how, questi infatti sono in grado di esplicitare e manifestare le informazioni dell'impresa in maniera percepibile e quindi anche opponibile verso i terzi soggetti esterni all'organizzazione, sotto forma, ad esempio, di dati e liste sui clienti e fornitori, piani aziendali, ricerche e strategie di mercato, conoscenze nell'utilizzo di software, processi e codici[74]; tuttavia vedremo nei prossimi capitoli come sempre più spesso il know-how dell'impresa venga conservato e quindi protetto in uno stato digitale, in quanto di più semplice e ottimale attuazione.

Già a partire da metà degli anni 80' si è qualificato il know-how come un "bene economico" capace di garantire al suo detentore la possibilità di utilizzare le informazioni in esso contenute in una forma esclusiva[75]. Ma un'ulteriore importante disciplina del know-how è stata attuata più recentemente con il decreto legislativo 11 maggio 2018, il quale ha introdotto nel nostro ordinamento la possibilità di iscrivere a bilancio il know-how segreto e riservato di un'impresa, più precisamente definibile come segreto commerciale, all'interno dei beni immateriali[76].

Le immobilizzazioni immateriali vengono definite dall'Organismo Italiano Contabilità 24 (da ora OIC) al paragrafo 9 come "*beni non monetari, individualmente identificabili, privi di consistenza fisica e sono, di norma, rappresentati da diritti giuridicamente tutelati*" e sono cioè un insieme di elementi che, attraverso l'avvio del processo produttivo, forniranno all'impresa un'entrata a lungo termine e contemporaneamente non sono dotate di fisicità, una

---

74 Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 14.

75 La qualificazione del know-how quale bene economico degno di tutela può essere rinvenuta nel pronunciamento Cass., 27 febbraio 1985, n. 1699, in G. CICCONE e F. GHINI, *La tutela giudiziale civile dei segreti commerciali anche dopo l'introduzione del d.lgs. n. 63/2018.* in *Dir. ind.*, 2019, V, 525. Si veda inoltre Cass., 20 gennaio 1992 n. 659 in *DeJure*. In questa sentenza viene definito il know-how quale: "Bene economico che assume rilievo come autonomo elemento patrimoniale, anche se derivi da invenzioni brevettabili che il titolare non intende brevettare e preferisce sfruttare in regime di segreto, o da ideazioni minori non costituenti, cioè, vere e proprie invenzioni, quindi, non brevettabili". Si veda ancora G. RESTA, (nt. 48), 276 e 337 dove viene indicato che il know-how, essendo un bene economico, può essere oggetto di cessione a titolo oneroso o gratuito. Il contratto di cessione può dunque consistere nel trasferimento del know-how da parte del titolare mediante una comunicazione a terzi delle conoscenze che lo costituiscono.

76 In tal senso si veda E. SALVATORE, *Know how - rivalutazione e patrimonializzazione del segreto commerciale - Un valore che non può andare perso,* Youcanprint, Lecce, 2020, 36 ss. Il valore economico dello stato di segretezza delle informazioni è rilevato anche nella sentenza della Cass., 28 giugno 1985, n. 3881, in E. SALVATORE, in cui si indica che: "Qualora il metodo adottato da un imprenditore, per realizzare determinati prodotti od applicazioni in favore dei clienti, manchi di esclusività e segretezza, il contratto di cessione di tale metodo (cosiddetta cessione di "know-how") resta privo di un oggetto economicamente apprezzabile".

simile indicazione di immobilizzazione immateriale può essere ritrovata all'interno dei principi contabili internazionali 38 (*International Accounting Standards Board,* da ora IAS)[77].

In generale, le attività immateriali sono classificate, secondo le disposizioni dell'OIC 24, in tre diversi gruppi nella macro-classe B.I. dell'attivo dello stato patrimoniale. L'art. 2424 c.c. indica che il know-how può essere iscritto in bilancio all'interno del secondo gruppo concernente i diritti sulle attività immateriali in due diverse voci, in base alle caratteristiche in esso presenti: nella voce B.I.3. "diritti di brevetto industriale e diritti di utilizzazione delle opere dell'ingegno" per know-how soggetto a tutela giuridica o all'interno della voce B.I.4. "concessioni, licenze, marchi e diritti simili" per costi di know-how classificati come tecnologia non brevettata.

Nella voce B.I.3. si possono contabilizzare elementi che rispondono a quanto disciplinato agli artt. 2584 ss. c.c. per ciò che riguarda i "diritti di brevetto", mentre per le opere dell'ingegno si fa riferimento a quanto stabilito all'art. 2575 c.c., si possono comprendere quindi nella voce B.I.3. i costi di produzione interna o esterna dei diritti di utilizzazione delle opere dell'ingegno, costi per l'acquisizione e la produzione di brevetti industriali, di brevetti per modelli utilità e disegni e modelli ornamentali, costi per i diritti in licenza d'uso di brevetti, costi relativi all'acquisto a titolo di proprietà o licenza di software applicativi a tempo determinato o indeterminato o ai sensi della legge sui diritti d'autore, infine come abbiamo già illustrato, possono includersi nella voce B.I.3. i costi di know-how*,* sia nel caso in cui questi siano sostenuti durante una produzione interna, sia nel caso vengano in essere acquisendo il know-how da terzi soggetti esterni, sempre se tutelati giuridicamente[78].

Nell'aggregato B.I.4. si fa invece riferimento sia a costi giuridicamente disciplinati come concessioni, licenze e marchi, sia a un aggregato residuale definito come "diritti similari", una

---

[77] Si veda M.S. AVI, *Il sistema informativo integrato, Volume I, Analisi aziendali di natura economico-finanziario: il bilancio come strumento di gestione,* Libreria Editrice Cafoscarina, 2019, 37 e come illustrato da M. FAZZINI in *Due Diligence 2019,* Ipsoa, 2019, 15, lo IAS 38, inerente le attività immateriali, non fornisce un elenco dettagliato degli *intangible* asset ma stabilisce i criteri per la loro identificazione. Secondo questo standard, un'attività è definibile come immateriale se: è separabile, ossia se può essere separata o scorporata dall'entità e venduta, trasferita, data in licenza, locata e scambiata, sia individualmente, che nell'insieme al relativo contratto, attività o passività; oppure è immateriale se deriva da diritti contrattuali o da altri diritti legali, indipendentemente dal fatto che tali diritti siano trasferibili, separabili dall'entità o da altri diritti e obbligazioni, in grado quindi di assicurare benefici economici futuri.

[78] Si veda M.S. AVI, (nt. 77), 95 ss. e A. QUAGLI, (nt. 73), 79. Nella voce BI3 dello stato patrimoniale sono contenuti i diritti di utilizzazione delle opere dell'ingegno al pari dei diritti sui brevetti. I diritti in esame rientrano nel novero dei beni immateriali veri e propri, sono rappresentati da diritti giuridicamente tutelati e perciò sono identificabili e individuabili secondo le disposizioni dell'OIC 24.

posta che possiamo indicare come non definita in modo analitico ma conforme a ciò che è disciplinato dall'art. 5 del d.lgs. 127/91, dove il legislatore indica che non è possibile *"escludere in una materia in continua evoluzione come quella dei diritti su beni immateriali, il sorgere di rapporti giuridici diversi da quelli oggi conosciuti"*. La voce B.I.4. può quindi comprendere costi per l'ottenimento di concessioni su beni di proprietà degli enti concedenti o per l'esercizio di attività proprie degli enti concedenti, costi per licenze di commercio al dettaglio, per l'acquisto di marchi, per la produzione interna di un marchio ed infine costi di know-how per una tecnologia che non risulti brevettata[79]. Ed è proprio la voce B.I.4. che appare più adeguata a contenere in bilancio il valore del capitale know-how dell'impresa tutelato come un segreto commerciale, in quanto non richiede particolari tutele giuridiche, come il brevetto previsto nella voce B.I.3., che peraltro comporterebbe l'eliminazione della caratteristica fondamentale di segretezza dell'informazione.

Il principio contabile internazionali 38 considera il know-how dell'impresa come "*intangible asset*", cioè bene privo di consistenza fisica e fonte di probabili benefici economici futuri, in questa specificazione ne ritroviamo una condivisione con i principi nazionali dell'OIC già illustrati precedentemente, si possono infine classificare l'assenza d'intangibilità, il carattere durevole, l'impiego nella fornitura di beni e servizi, la capacità di valutare tali beni a livello di futuri proventi economici, tutti tratti distintivi del know-how presenti sia nelle disposizioni dell'OIC che nelle disposizioni internazionali dello IAS 38.

Il know-how, dato il suo valore economico intrinseco, può essere ulteriormente trasmesso attraverso una licenza d'uso: tale licenza, come già illustrato, è un importante parametro di valutazione dell'indennizzo nel caso di un utilizzo illecito di un segreto commerciale[80]. Il valore economico del segreto commerciale è sicuramente un elemento fondamentale, troviamo una prova di ciò nel richiamo ad uno dei tre requisiti richiesti all'articolo 98 c.p.i. Ricordiamo infatti che le informazioni per essere tutelate come segreto commerciale devono avere un valore economico in quanto segrete (si veda *supra* 1.3.1.).

Si riscontra tuttavia una problematica nell'individuare le modalità di valutazione e rivalutazione di tale valore, in particolare in presenza di beni che abbiamo definito intangibili.

---

[79] In tal senso si veda A. QUAGLI, (nt. 73), 95.

[80] Come disposto dall'art. 124 c.p.i., co. 6-*quater*, c.p.i.: "L'indennizzo liquidato a norma del comma 6-*ter* non può, in ogni caso, superare l'importo dei diritti dovuti qualora la parte istante avesse richiesto l'autorizzazione ad utilizzare i segreti commerciali per il periodo di tempo per il quale l'utilizzo degli stessi avrebbe potuto essere vietato".

Le disposizioni dello IAS 38 prevedono due sistemi di valutazione del know-how*:* un modello di costo, con successive diminuzioni di ammortamenti e svalutazioni, e un modello definito come "rideterminazione del valore iniziale", che viene assoggettato a successive rivalutazioni secondo il cosiddetto metodo del "*fair value*". Il metodo *fair value* stabilisce il valore del bene intangibile al netto di qualsiasi successivo ammortamento accumulato (fondo ammortamento) e di qualsiasi successiva perdita per riduzione di valore accumulata o svalutazioni in base a parametri e indici scaturiti da un mercato attivo. La bassa diffusione di mercati attivi dei beni intangibili ha richiesto però approfondimenti del criterio di valutazione al *fair value*, nell'ambito del quale lo IASB ha previsto ulteriori tecniche di valutazione del know-how*,* come il "*market approach*", il "*cost approach*" e "*l'income approach*"[81].

Nel sistema di valutazione dei bene immateriali la disciplina dello IAS 38 presenta alcune differenze rispetto i principi contabili nazionali stabiliti dall'OIC 24, in quest'ultima viene infatti indicata la sola applicazione del metodo del costo storico come sistema per la valutazione in bilancio dei beni immateriali e quindi dei segreti commerciali, con limite identificabile nel valore recuperabile, mentre la rivalutazione delle voci è possibile solo in caso di leggi speciali che ne stabiliscono le metodologie da adottare e i limiti entro cui la rivalutazione potrà essere effettuata[82].

Il recente documento interpretativo n. 7 dell'OIC, avente per oggetto il trattamento contabile della rivalutazione dei beni da effettuare ai sensi dell'art. 110 d.l. 104/2020, ha stabilito che anche i beni immateriali mai iscritti nello stato patrimoniale, in quanto i relativi costi sono sempre stati imputati a conto economico, possono essere rivalutati e iscritti nell'attivo patrimoniale a condizione che tali beni siano giuridicamente tutelati alla data di chiusura del bilancio. Tra questi beni potenzialmente rivalutabili va ricompreso quindi il kwow-how

---

[81] Lo IASB, il 12 Maggio 2011, con effetti dirimenti sulla questione della valutazione al *fair value*, ha emanato l'IFRS 13 rubricato: "Valutazione del Fair Value", pubblicato nella Gazzetta Ufficiale dell'Unione Europea nel dicembre del 2012. Si veda E. SALVATORE, (nt. 76), 37. Sintetizzando il funzionamento dei tre diversi metodi di calcolo del *fair value,* possiamo indicare che: nel *market approach* si distingue i prezzi standard con le analogie comparative, calcolando il *fair value* sui valori di mercato, nell'*income approach,* si valuta il potenziale reddito aziendale, determinando diverse leve così da stimare il reddito attuale, mentre nel *cost approach* si determina il valore corrente attraverso due approcci, quello della sostituzione e quello che si basa sui costi di produzione.

[82] Come indicato dall'art. 2426, co. 1, n.1 c.c.: "Le immobilizzazioni immateriali devono essere iscritte in bilancio al costo di acquisto o produzione", A. QUAGLI, (nt. 73), 97, aggiunge che la valutazione al costo di acquisto comprende anche tutti gli oneri accessori, mentre la valutazione al costo di produzione, oltre ai costi direttamente imputabili, include gli eventuali costi indiretti per la quota ragionevolmente imputabile all'immobilizzazione. Per ciò che concerne i limiti al valore di iscrizione A. QUAGLI, (nt. 73), 98, sottolinea che ciò è limitato dal c.d. "valore ricuperabile". Se il valore di iscrizione risultasse perciò superiore al valore recuperabile, l'immobilizzazione dev'essere iscritta a quest'ultimo valore. Nel documento OIC 9 viene definito il valore recuperabile come il maggiore tra il *fair value* al netto dei costi di vendita o il valore d'uso.

aziendale, declinato anche nella qualifica di segreto commerciale[83].

La rivalutazione tuttavia rimane un procedimento complesso, al fine di scongiurare eventuali e possibili contestazioni ad opera degli organi di controllo o revisori e per non ricorrere a redazioni di bilanci non veritieri e corretti e quindi passibili di integrare gravi reati quale il falso in bilancio, in merito alla quantificazione del valore dell'intangibile può essere opportuno ricorrere allo strumento della certificazione del valore del bene intangibile operata da un apposito ente di certificazione.

[83] In tal senso si veda il documento Interpretativo n. 7, Legge 13 ottobre 2020, n. 126, "aspetti contabili della rivalutazione dei beni d'impresa e delle partecipazioni" in cui si stabilisce che: "Possono essere oggetto di rivalutazione i beni immateriali ancora tutelati giuridicamente alla data di chiusura del bilancio in cui è effettuata la rivalutazione anche se i relativi costi, seppur capitalizzabili nello stato patrimoniale, sono stati imputati interamente a conto economico". Si veda in tal senso anche E. SALVATORE, (nt. 76), 128.

CAPITOLO 2. CONFRONTO TRA I DIRITTI DI PROPRIETÀ INDUSTRIALE E INTELLETTUALE

SOMMARIO: 2.1. Il brevetto - 2.2. Modelli di utilità - 2.3. Disegni e modelli - 2.4. I diritti d'autore - 2.5. Cumulazione e integrazione dei diritti di proprietà - 2.5.1. Le relazioni tra segreti commerciali e i brevetti - 2.5.2. Il caso dei software.

2.1. Il brevetto

Il brevetto è un istituto giuridico che assicura all'inventore il diritto "di utilizzazione" esclusiva dell'invenzione per un certo periodo di tempo. Le invenzioni che possono essere tutelate sono però circoscritte all'alveo del settore tecnologico, ossia invenzioni considerate come "industriali". Nella normativa civilistica manca ancora una definizione specifica di invenzione, da cui si ricava la possibilità di valutare come un possibile dato aperto, cioè suscettibile di accogliere al proprio interno diverse realtà che potrebbero venir definite come una soluzione originale in grado di risolvere un problema tecnico o di migliorare eventuali standard prestazionali riguardante procedimenti o prodotti principali, ovvero indipendenti rispetto ad altre invenzioni presenti[84].

Il brevetto può essere presentato come un diritto negativo, in quanto esclude ad altri soggetti, diversi dall'inventore, l'utilizzo della tecnologia brevettata, e svolge un duplice importante ruolo: il brevetto è sia un incentivo ad innovare, dato che concede all'inventore una protezione e un'esclusività di utilizzo che può essere fonte di vantaggio competitivo, ma allo stesso tempo è un incentivo a condividere, in quanto il titolare del brevetto risulta obbligato a pubblicare i dettagli dell'invenzione per poter ottenere l'esclusiva. Il brevetto può essere così rappresentato come un "contratto" tra inventore e collettività[85], in quanto permette all'inventore di tutelare le proprie invenzioni con la nascita di diritti di esclusiva sulla tecnologia brevettata, in cambio permetta l'acquisizione di informazioni da parte della

---

[84] Come indicato nella regola 42, co. 1, lett. c, del regolamento di esecuzione della CBE. In tal senso si veda G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 382. Tale indicazione non definisce specificamente cosa debba intendersi per invenzione oggetto di brevetto, la scelta del legislatore suggerisce che l'invenzione dev'essere intesa come un concetto aperto, caratterizzato da una ricettività praticamente illimitata.

[85] Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 367 ss., C. GARUFI, (nt. 42), 27. e G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 380. In particolare quest'ultimo autore sottolinea l'importanza del meccanismo della pubblicità, in quanto rende accessibili alla collettività i risultati dell'attività di ricerca, contribuendo agli interessi tutelati dall'articolo 9 della Costituzione.

collettività su una determinata invenzione grazie ad una logica di rivelazione.

Il brevetto, come le altre norme in materia di proprietà intellettuale e industriale, si fonda su un principio di territorialità dell'estensione della protezione: le imprese hanno la facoltà di decidere su che territorio estendere il diritto di privativa che svolge la sua efficacia in relazione alla tipologia di deposito del brevetto e all'ufficio alla quale viene inoltrata la domanda, determinandone i confini entro i quali valgono le tutele degli interessi del titolare del diritto: esistono infatti brevetti di portata e tutela nazionale, di competenza dell'Ufficio Italiano Brevetti e Marchi (da ora UIBM), europea, di competenza dell'European Patent Office (da ora EPO) e internazionale, di competenza del World Intellectual Property Organization (da ora WIPO). Di seguito tratteremo la disciplina del brevetto nazionale, anche alla luce del fatto che il brevetto europeo non è ancora, ad oggi, un vero e proprio brevetto unitario e sopranazionale, ma può essere definito più come un fascio di brevetti nazionali, dove unificata è la sola procedura, e dato che la disciplina si presenta attualmente molto simile, almeno per gli aspetti essenziali, alla normativa nazionale[86].

I requisiti di brevettabilità richiesti ad un invenzione sono quattro: la novità, intesa come la caratteristica dell'invenzione di non essere compresa nello stato della tecnica o nello stato dell'arte come stabilito dall'art. 46 c.p.i., l'originalità, ossia il fatto che l'invenzione non deve

---

[86] Si veda C. GARUFI, (nt. 42), 40 e A. VANZETTI, V. DI CATALDO, (nt. 48), 377 ss. L'entrata in vigore del brevetto europeo con effetto unitario, che non sostituirà ma semplicemente affiancherà la tutela brevettuale esistente a livello nazionale e a livello europeo, è oggi prevista per il 2022. Sono slittati e ancora incerti i tempi di attuazione del brevetto europeo, questo a causa di due fattori: il ritardo nella ratifica dell'accordo TUB da parte della Germania e la Brexit. Per maggiori informazioni si veda il sito ufficiale dell'EPO. Si veda inoltre B. CALABRESE *Preminenza del brevetto europeo e autonomia del brevetto italiano,* in *Giur. comm.*, 2020, III, 576, in cui, commentando la Cass., 16 settembre 2019, n. 22984, si specifica che con questa sentenza la Corte di Cassazione è intervenuta per sancire un principio di diritto specifico, ma non per questo di rilevanza secondaria, riguardante i rapporti di validità ed efficacia tra brevetto europeo e italiano. Tali rapporti sono alla base dell'organizzazione brevettuale stabilita dalla Convenzione di Monaco, la cui complessità verrà ulteriormente incrementata dal regime ad effetto "unitario" di futura applicazione nel 2022, all'esito di un *iter* normativo nel contesto dell'UE, che come abbiamo già indicato, ancora oggi non del tutto compiuto e che si può definire tranquillamente "travagliato". È proprio tale complessità sistematica a segnare l'importanza della pronuncia della Cassazione, che pone ordine ad una materia dall'elevato tecnicismo, che la stessa giurisprudenza italiana di merito, pur in sede di sezione specializzata, dimostra di valutare con una certa difficoltà. Per ciò che riguarda il criterio di preminenza del brevetto europeo, ovvero il divieto di cumulo con il brevetto nazionale italiano, la questione giuridica ruota attorno al c.d. "criterio di preminenza" del brevetto europeo rispetto al brevetto italiano, come disciplinato dall'art. 59 c.p.i. Ai sensi di tale normativa, quindi, l'eventuale coincidenza tra i due brevetti a tutela della medesima invenzione è risolta a favore del brevetto europeo, determinando così l'inefficacia del brevetto nazionale italiano. La sovrapposizione tra titoli diversi a livello territoriale, ma coincidenti per contenuti e attribuzioni, è però possibile per la peculiare architettura del sistema brevettuale. Il brevetto europeo è infatti un brevetto di portata internazionale, il quale beneficia di una disciplina convenzionale comunitaria, tuttavia, esso non elimina la parallela esistenza dei regimi brevettuali nazionali. Oltre a ciò, il brevetto europeo, pur essendo a rilascio centralizzato presso il competente ufficio sovranazionale dell'EPO, completa il suo *iter* di pubblicazione attraverso una dimensione nazionale; l'erronea espressione secondo cui il brevetto europeo si risolve in un "fascio di brevetti nazionali" secondo l'autore sarebbe dunque determinata proprio dall'*iter* di pubblicazione del brevetto comunitario.

risultare, per una persona esperta del settore, evidente dallo stato della tecnica come disciplinato all'art. 48 c.p.i., l'industrialità, ossia caratterizzante da un invenzione di prodotto (con caratteristica intrinseca la fabbricabilità) o di processo (con una possibile utilizzabilità industriale) come indicato all'art. 49 c.p.i., infine l'art. 50 c.p.i stabilisce che l'invenzione dev'essere lecita, non contraria quindi a ordine pubblico o buon costume. Se comunque almeno un uso è lecito l'invenzione può essere considerata lecita e quindi brevettabile[87].

Il brevetto ha una durata ventennale, il calcolo della durata di tutela inizia dalla data di deposito presso l'UIBM, i diritti nascenti dall'invenzione industriale non possono tuttavia essere rinnovati né prorogati e, nel caso di brevetto italiano, sono limitati al territorio nazionale come stabilito dal principio di territorialità già illustrato precedentemente. I diritti collegati all'invenzione sono innanzitutto il diritto ad essere riconosciuto come inventore, che resta sempre in capo alla persona fisica che ha inventato il prodotto, il metodo o il procedimento e che ha diritto a richiederne: questi diritti sono personali e di natura morale e si differenziano dai diritti di esclusiva di utilizzo che nascono con il rilascio del brevetto, che sono invece di natura patrimoniale, alienabili e rinunciabili, valutabili quindi come un possibile diritto di tipo negativo[88].

---

[87] Per una trattazione più approfondita dei requisiti di brevettabilità si veda G. GHIDINI, G. CAVANI, (nt. 27), 16 e G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 387 ss. Evidenziando solamente i tratti principali dei requisiti, si determina per novità la risoluzione di un problema mediante una soluzione tecnica innovativa e meno costosa, si incentiva così il progresso innovativo scientifico e tecnico. L'art. 46 c.p.i. definisce nuova l'invenzione che non è compresa nello stato della tecnica, si configura così il requisito di novità estrinseca in termini assoluti e universali rispetto conoscenze già note. L'attività inventiva dell'invenzione è dunque intesa come una conoscenza nuova, superiore alle normali evoluzioni della tecnica; più precisamente essa "segna la linea di confine fra ciò che appartiene al divenire normale di ciascun settore, che potrebbe essere realizzato da qualunque operatore e che, quindi non merita la protezione, e ciò che invece è frutto di un'idea che supera le normali prospettive di evoluzione del settore, che non è alla portata dei tanti che in esso operano e che, quindi, merita la tutela esclusiva", come disposto dal Trib. Roma, 12 settembre 2001, in *GADI*. Il secondo requisito richiesto è l'originalità, l'invenzione deve portare ad una nuova conoscenza, superiore alla normale e quotidiana evoluzione della tecnica. Il terzo requisito per la validità dell'invenzione è l'industrialità, che deve essere presente o nelle fase di fabbricazione o in quella di utilizzazione dell'invenzione. La prima alternativa si riferisce all'invenzione c.d. di prodotto, la seconda a quella di procedimento: come ad esempio la macchina utensile ed il c.d composto intermedio. Infine, trattando il quarto requisito di brevettabilità, ossia la liceità, si sottolinea che questo è un requisito che solo recentemente ha acquisito un certo spessore. Sono contrarie al requisito di liceità tutte le invenzioni la cui attuazione è contraria all'ordine pubblico o al buon costume, sebbene costituiscono vere e proprie invenzioni, dotate, in linea di principio, di tutti gli altri requisiti indispensabili per la concessione della privativa. La *ratio* dell'esclusione dalla brevettabilità si basa sul sistema di valori in cui è fondata la società come apparendo così estranea ad una considerazione propria della disciplina brevettuale.

[88] In tal senso si è espresso G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 387 ss, il quale analizzando i diritti morali si sostiene che tale diritto "tutela l'inventore a godere della stima della comunità". Questo diritto è inalienabile e irrinunciabile, riflette inoltre in generale il diritto al riconoscimento della paternità delle proprie azioni, rientrando nella categoria dei diritti inviolabili della persona, come disposto nell'art. 2 Cost. Perciò il diritto di brevetto tutela interessi eterogenei che ricomprendono sia l'interesse alla tutela che alla remunerazione del lavoro di ricerca, rispondendo a tutti quegli interessi di remunerazione degli investimenti imprenditoriali sostenuti per le attività di ricerca e innovazione. Questi interessi trovano pure un fondamento Costituzionale, agli artt. 45 e 41.

Nella domanda di brevetto è necessario presentare una descrizione dettagliata dell'invenzione in modo da permettere ad una persona esperta del settore l'attuazione dell'invenzione stessa, sono necessari disegni che illustrino in maniera puntuale la forma e l'architettura dell'invenzione, deve essere ulteriormente indicati una serie di rivendicazioni. Le rivendicazioni sono fondamentali in quanto determinano l'area su cui si applicherà il diritto di esclusiva d'uso dell'invenzione, ciò comporterà il divieto ad altri soggetti di sfruttare e riprodurre l'idea, evocando così un carattere di opponibilità *erga omnes* del diritto, indirizzando inoltre la tutela verso un utilizzo esclusivo dell'innovazione al suo titolare per un periodo di tempo determinato. Questo diritto d'esclusiva si potrà applicare su un certo prodotto, si parlerà quindi di brevetto di prodotto, o su di un procedimento, in questo caso l'esclusiva riguarderà sia i prodotti ottenuti dal processo, sia le tecniche di produzione o di realizzazione e si indicherà come brevetto di procedimento[89].

L'invenzione potrebbe richiedere, per la sua realizzazione, l'uso di un procedimento o di un prodotto coperto da un brevetto anteriore, si parlerà quindi di invenzione dipendente, che può essere di perfezionamento o di combinazione con il prodotto coperto da brevetto anteriore. Il titolare dell'invenzione dipendente, per realizzare la propria tecnologia, ha la necessità di ottenere il consenso per l'utilizzo da parte del titolare del brevetto anteriore al quale la sua invenzione è collegata. In ogni caso, entro certi limiti, il titolare dell'invenzione dipendente è favorito dalla presenza di una licenza obbligatoria nel caso in cui il titolare del brevetto anteriore non concedesse la licenza in maniera volontaria.

L'art. 45, co. 4, c.p.i. disciplina le invenzioni che non possono essere tutelabili come brevetto: queste sono le scoperte puramente teoriche, che si differenziano dall'invenzione per la distanza dallo scopo pratico, le teorie scientifiche e i metodi matematici, i piani, i principi ed i

---

[89] Per ciò che riguarda l'opponibilità *erga omnes* del diritto, si veda C. GARUFI, (nt.42), 27, il quale sostiene che per molti aspetti nel brevetto è richiamata la disciplina in materia di monopolio, che garantisce una tutela meno pregnante rispetto quella della proprietà. Tuttavia in senso contrario si esprime A. VANZETTI, V. DI CATALDO, (nt. 48), 372 ss, in cui, illustrando la funzione del brevetto, tra monopolio e concorrenza, si esclude che l'idea del brevetto crei dei veri e propri monopoli, e quindi non svolga, nel suo complesso, un ruolo positivo per il sistema economico. Secondo l'autore oggi prevale l'idea che vede nel brevetto una valenza positiva, ciò ha portato ad un'estensione mondiale praticamente illimitata dei sistemi brevettuali. In tal senso si esprime anche G. GHIDINI, G. CAVANI, (nt. 27), 3. Si aggiunge inoltre che, ad oggi, è universalmente riconosciuto che il brevetto gioca un ruolo positivo solo all'interno di un sistema di libero mercato, perché in un sistema di mercato gli effetti positivi del brevetto, come il suo ruolo nell'incentivare l'innovazione, superano gli effetti negativi, dati dalla sua struttura monopolistica. Viceversa, in sistemi non di libero mercato, come quelli presenti in molti paesi in via di sviluppo, la sola incentivazione all'innovazione è un principio che ha un peso minore, così facendo gli effetti monopolistici potrebbero non essere adeguatamente compensati positivamente. Il sistema brevettuale, essendo un sistema complesso, può dunque fatalmente essere soggetto a imperfezioni causate da mutamenti legati a fenomeni economici, tecnologici, sociali, ed è quindi necessario adattare il sistema alle mutazioni ambientali, senza eliminare completamente la funzione dell'istituto, come sostenuto da G. GHIDINI, G. CAVANI, (nt. 27), 3.

metodi per attività intellettuali, come metodi di studio o insegnamento e analisi, sistemi di spiegazioni, codici di catalogazione, metodi di controllo della produzione, diete alimentari, progetti di ingegneria, metodi utilizzati per scopi di gioco o per attività commerciale, come idee imprenditoriali, metodi pubblicitari, tecniche contabili, non sono tutelabili come brevetti neanche i programmi di elaboratore, i quiz o le pubblicità, le presentazioni di informazioni quali l'allestimento di tabelle o scale[90].

In aggiunta l'art 45, co. 4, c.p.i. illustra che non sono brevettabili i metodi per il trattamento chirurgico come attività cruente su un organismo vivente, con finalità puramente estetiche quali gli interventi di chirurgia plastica o distruttive, le tecniche di sterilizzazione o trattamenti terapeutici, come attività ausiliarie alla chirurgia con finalità curative, metodi di diagnosi applicati al corpo umano e animale; sono invece brevettabili i prodotti utilizzabili durante il procedimento. Non sono brevettabili le razze animali, i procedimenti essenzialmente biologici che prevedano la produzione di animali o vegetali, sono invece brevettabili i micro-organismi e i procedimenti che si avvalgono di questi, come un vaccino o un processo OGM[91].

Ulteriori esclusioni a possibili tutele come brevetti vengono indicate dall'art. 81-*quinquies* c.p.i., che dispone che sono esclusi dalla brevettabilità il corpo umano sin dal momento del concepimento e la sequenza parziale del gene, le invenzioni contrarie alla dignità umana, all'ordine pubblico e al buon costume, come la clonazione umana, lo screening genetico, l'utilizzo di cellule embrionali, i procedimenti di modificazione dell'identità genetica degli animali, infine non sono mai brevettabili ogni tipo di procedimento che prevede l'utilizzo di cellule embrionali umane[92].

---

[90] Come indicato da A. VANZETTI, V. DI CATALDO, (nt. 48), 380 ss. e G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 382, in questi casi si presenta una diversa *ratio* dell'esclusione alla brevettazione, che risulta unitaria e consiste nella carenza dell'industrialità nel momento di attuazione, quindi nel contenuto dell'oggetto dell'invenzione. Il carattere di questi casi è meramente intellettuale, perciò non si presentano, nel momento della loro costruzione, quel carattere tecnico che distingue l'invenzione dalla mera scoperta.

[91] Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 386 e G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 386, in cui si illustra che l'art. 45, co. 4, c.p.i., riprende l'art 52.4 CBE, dove si stabilisce che i metodi per il trattamento chirurgico o terapeutico del corpo umano o animale ed i metodi di diagnosi non sono brevettabili in quanto privi del carattere di industrialità.

[92] Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 386 ss. G. ANGELICCHIO in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 386, commentando l'articolo gli autori evidenziano come la *ratio* del divieto è collegata all'opportunità di non consentire privative su mere forze naturali, che sarebbero prive di un carattere prettamente tecnico o industriale. Il rigore dell'esclusione dalla tutela brevettuale sarebbe però attenuata dalla previsione secondo cui tale limitazione non si applica a procedimenti microbiologici ed a prodotti ottenuti mediante tali procedimenti. Questa disposizione distingue dunque la nozione di microrganismo da macrorganismo, che tuttavia le progressive scoperte nell'ingegneria genetica hanno sostanzialmente ridotto.

2.2. Modelli di utilità

Differentemente dalle disposizioni della disciplina europea in tema di brevettazione, il nostro ordinamento all'art. 82 c.p.i. ha previsto un'ulteriore forma di tutela all'innovazione tecnica, sempre per invenzioni che presentino un carattere industriale, anche come modelli di utilità, nel caso in cui una "*particolare efficacia e comodità di applicazione o di impiego*" sia data da una forma nuova di un prodotto industriale, in particolare, sono oggetto di tutela come modelli d'utilità quelle forme di prodotto consistenti in particolari conformazioni, disposizioni, configurazioni o combinazioni di parti. Non esistono attualmente i modelli d'utilità in tutti gli Stati membri dell'UE e la protezione garantita da tale istituto non può essere ottenuta a livello comunitario. La tutela dell'invenzione come modello d'utilità ha validità dieci anni e non è rinnovabile, la domanda dev'essere effettuata presso l'UIBM presentando una descrizione dell'invenzione che sia sufficiente ad attuarla. Il processo di registrazione ha una serie di vantaggi, in quanto risulta più economico, celere e semplice rispetto quello necessario per il brevetto per invenzione. L'UIBM eseguirà infatti solo delle verifiche degli aspetti formali senza sottoporre il modello d'utilità a una ricerca di novità come invece previsto per il brevetto per invenzione, non emettendo rapporti di ricerca né opinioni di brevettabilità. Ulteriore differenza sostanziale rispetto al brevetto è che la tecnologia tutelata come modello utilità non è necessariamente una risposta ad una soluzione nuova ad un problema specifico o tecnico; non risulta comunque facile la demarcazione tra modelli utilità e brevetto, tant'è che alcuni paesi definiscono i modelli d'utilità come "brevetti minori" o come "piccole invenzioni"[93].

---

[93] Si veda G. GHIDINI, G. CAVANI, (nt. 27), 61 e A. VANZETTI, V. DI CATALDO, (nt. 48), 521 ss. e M. FAZZINI in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 482 ss. in cui si presenta il modello utilità e la sua possibile armonizzazione ed unificazione a livello comunitario, cosa che ad oggi non è stata ancora attuata. Si specifica inoltre che la sostanziale qualificazione del modello d'utilità come "invenzione minore" sarebbe intesa come un'invenzione dotata di un minore livello di attività inventiva. La *ratio* dell'introduzione del modello d'utilità nell'ordinamento italiano sarebbe quindi volta a riconoscere una tutela ad una categoria di invenzioni minori. Una volta concluso l'esame preventivo di novità si riconosce agli inventori la possibilità di ottenere il brevetto senza altri esami, ulteriori formalità potrebbero infatti essere ritenute un dispendio troppo eccessivo rispetto all'importanza dell'invenzione stessa. Si veda ancora il sito ufficiale dell'EUIPO, voce modelli d'utilità, dove vengono descritti i modelli di utilità come un diritto esclusivo concesso per un'innovazione, simile a un brevetto, che talvolta è chiamato "brevetto a breve scadenza" o "brevetto di innovazione". Il brevetto per modello di utilità può essere concesso a chiunque inventi o scopra macchinari, prodotti, composizioni di materia o nuovi e utili miglioramenti degli stessi. Nel documento *IPTK Basics,* 2014, 67, redatto dall'EUIPO e pubblicato dall'UEB Monaco, si presentano i modelli d'utilità come diritti di proprietà intellettuale che proteggono le invenzioni tecniche, proprio come i brevetti. A differenza però dai brevetti, i modelli di utilità sono disponibili solo in alcuni paesi, per esempio in Austria, Cina, Germania e Giappone, ma non in altri, come in Canada, Regno Unito e USA. Un'altra differenza che si riscontra sta che, nella maggior parte dei paesi, i requisiti sostanziali, come novità, implicazione di un'attività inventiva, applicabilità industriale, non sono esaminati nel momento in cui un modello di utilità viene registrato e pubblicato. Come quindi i disegni o modelli registrati, i marchi registrati, i modelli di utilità costituiscono diritti di proprietà intellettuale registrati parzialmente e non esaminati.

Perché l'invenzione possa essere protetta come modello utilità è necessario che la tecnologia presenti una serie di requisiti: dev'essere nuova e originale, deve cioè avere un'efficacia particolare o un certo impiego nel senso di originalità con elementi innovativi caratterizzanti.
Come stabilito dall'art. 82 c.p.i. possono costituire invenzioni tutelabili come modello d'utilità: "*Macchine o parti di esse, strumenti, utensili ovvero oggetti di uso in genere, quali i nuovi modelli consistenti in particolari conformazioni, disposizioni, configurazioni o combinazioni di parti*"*;* sono esclusi invece dalla tutela come modello utilità procedimenti industriali, invenzioni chimiche, biotecnologiche ed elettroniche[94].
L'imprenditore interessato alla tutela della propria innovazione tecnologica può richiedere la domanda sia di brevetto per un'invenzione industriale che per brevetto come modello d'utilità, come stabilito dall'art. 84 del c.p.i., la domanda del modello d'utilità avrà "*da valere solo nel caso che la prima non sia accolta o sia accolta solo in parte*"; Si tratta quindi di domande alternative, perciò nel caso in cui l'imprenditore non riuscisse ad ottenere la tutela come brevetto per invenzione industriale potrà sempre far valere la tutela dell'invenzione come modello utilità. Il livello di tutela risulterà pressoché equivalente a quello conferito ai brevetti ma con una durata inferiore di dieci anni rispetto i venti del brevetto[95].

---

[94] Si veda il sito ufficiale del Ministero dello Sviluppo Economico, *Disegni e modelli,* 2021 e D.U. SANTOSUOSSO in *Commentario del codice civile, delle società dell'azienda della concorrenza, art. 2575-2642,* Utet Giuridica, 2014, 416, il quale, esponendo i requisiti richiesti dal 82 c.p.i., definisce che per nuovo s'intendono tutti i modelli non anticipati da alcuna predivulgazione e da alcuna anteriorizzazione. Non si considerano perciò nuovi i modelli d'utilità che sono già stati oggetto di comunicazione e che possono quindi essere riprodotti, o che sono stati oggetto di vendita, anche con un limitato numero di esemplari, che sono stati descritti su articoli di stampa o su media specializzati, oppure infine che sono stati oggetti di una precedente domanda di registrazione. Per ciò che concerne il principio di originalità D.U. SANTOSUOSSO specifica che questo principio è presente in modelli che realizzano un progresso consistente rispetto alla realtà esistente, con un criterio quindi differente da quello previsto in tema di brevetto.

[95] Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 524. L'art. 84 c.p.i precisa che è "consentito a chi chiede il brevetto per invenzione industriale, di presentare contemporaneamente domanda di brevetto per modello di utilità, da valere nel caso che la prima non sia accolta o sia accolta solo in parte. Se la domanda ha per oggetto un modello anziché un'invenzione o viceversa, l'UIBM invita l'interessato, assegnandogli un termine, a modificare la domanda stessa, la quale tuttavia ha effetto dalla data di presentazione originaria. Se la domanda di brevetto per modello di utilità contiene anche un'invenzione o viceversa, è applicabile l'articolo 161". Si veda anche D.U. SANTOSUOSSO, (nt. 94), 417, in cui, presentando l'art. 84 c.p.i, sottolinea come la disciplina del modello di utilità ha molti punti di contatto e di contiguità con la disciplina del brevetto, tant'è che, come disposto dall'art. 84 c.p.i., è chiaro come l'oggetto del brevetto possa essere spesso valutato sotto le due diverse prospettive, con possibile successo alternativo. Per questa ragione l'inventore può depositare entrambe le domande, così da ottenere, in ogni caso, sussistendone gli estremi e tutti i requisiti richiesti, almeno una delle due registrazioni. Laddove però una domanda di registrazione presenti certi elementi di nullità, in quanto la qualificazione giuridica data all'invenzione non coincide con quella che giuridicamente gli si può legittimamente attribuire, l'UIBM concede immediatamente il diritto a modificare il contenuto della domanda di registrazione stessa, come da invenzione a modello di utilità, oppure viceversa, al fine di ottenere una registrazione che risulta comunque valida. G. GHIDINI, G. CAVANI, (nt. 27), 61. Tuttavia si puntualizza che non è possibile convertire invenzioni che non riguardano la forma di un prodotto, come ad esempio un procedimento, ad un'invenzione a contenuto chimico o biotecnologico o essenzialmente elettronico, come disciplinato agli artt. 87-97 c.p.i.

2.3. Disegni e modelli

Una forma di tutela disciplinata dal nostro ordinamento per particolari forme esterne di un prodotto è il disegno o modello. Questa forma di protezione può essere applicata a una qualsiasi forma esteriore di un prodotto o di una parte di un prodotto di origine artigianale e industriale che presenta elementi originali e/o capricciosi. L'art 31 c.p.i. definisce come disegno e modello *"l'aspetto dell'intero prodotto o di una sua parte quale risulta, in particolare, dalle caratteristiche delle linee, dei contorni, dei colori, della forma, della struttura superficiale e/o dei materiali del prodotto stesso e/o del suo ornamento"*[96].

Queste forme devono presentare determinate condizioni: come stabilito dall'art. 32 c.p.i., la forma estetica dev'essere nuova, non dev'essere stata perciò precedentemente divulgata o essere presenti elementi identici o con dettagli rilevanti simili ad altre forme già divulgate da altri, deve inoltre mostrare un carattere individuale, come sancito dall'art. 33 c.p.i., suscitando nell'utilizzatore informato un'impressione individuale diversa rispetto i prodotti già presenti sul mercato[97]. L'art. 31, co. 2, c.p.i., definisce che possono essere registrati come modelli tutti i "*componenti che devono essere assemblati per formare un prodotto complesso smontato o rimontato",* dove per prodotto complesso s'intende un prodotto formato da più elementi che può essere sostituito, o ancora *"gli imballaggi, le presentazioni, i simboli grafici e caratteri tipografici, esclusi i programmi per elaboratore*"[98].

La disciplina dell'art. 37 c.p.i. prevede un periodo di protezione di cinque anni a decorrere dalla data di presentazione della domanda, prorogabile fino a una durata massima di venticinque anni dalla data di registrazione. Per il principio di territorialità la domanda di

---

[96] Si veda F. SANNA in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 348 ss, in cui si indica che la tradizionale bipartizione che vede contrapposti disegni e modelli industriali compare nel testo italiano della d. CE 98/71, da traduzione del temine inglese "*design*", il quale comprende sia i c.d. disegni bidimensionali che i modelli tridimensionali.

[97] La nuova disciplina inerente i disegni e modelli ha previsto una serie di casi di predivulgazione accettate, le quali non pregiudicano quindi la tutela come disegno e modello. Sono ammesse ipotesi di predivulgazione come nel caso di: comunicazioni a terzi vincolati a segreto, divulgazioni dovute ad abuso di danni verso l'autore del disegno, le divulgazioni che non abbiano raggiunto ambienti specializzati del settore o divulgazioni eseguite dall'autore dodici mesi prima la data della domanda registrazione, si costituisce così un periodo di grazia. Nell'accertare il carattere individuale si valuta l'affollamento del settore: tanto più limitata è la libertà del designer, tanto più basteranno minori differenze per determinare immagini o idee diverse di prodotti; il prodotto potrà così essere registrato come disegno e modello. Si veda G. GHIDINI, G. CAVANI, (nt. 27), 62.

[98] Sono numerose le possibili tipologie di forme registrabili come disegni e modelli, *IPTK Basics* dell'EUIPO, (nt. 93), 54, descrive che tale istituto giuridico costituisce l'aspetto ornamentale o estetico di un articolo industriale, in elementi tridimensionali, come: la forma di un articolo, elementi bidimensionali, modelli, linee o colori. Solo per citarne alcuni, possono costituire elementi estetici di un disegno o modello: linee, colori, ornamenti, forme, strutture, contorni e materiali, o tutti gli altri elementi capaci di rendere il prodotto nuovo e con un certo carattere individuale.

registrazione di un disegno e modello all'UIBM determina la valenza della tutela all'interno del solo territorio italiano, la domanda può comunque venir inoltrata anche all'European Union Intellectual Property Office (da ora EUIPO) così da estendere la protezione all'interno di tutto il territorio della Comunità Europea, oppure l'imprenditore potrà chiedere anche una tutela in più paesi stranieri presentando domanda presso il World Intellectual Property Organization (da ora WIPO). La domanda di registrazione può essere effettuata per un solo disegno e modello o per più disegni e modelli anche se presentanti leggere differenze, in tal caso si parla di deposito plurimo o multiplo[99].

Con la registrazione del disegno e modello l'autore ha un diritto esclusivo di utilizzo e può vietarne l'uso a terzi per atti quali l'esportazione, l'importazione, la fabbricazione, la commercializzazione e l'offerta. La tutela si estenda anche alla contraffazione di carattere non dolosa o colposa di sviluppo di disegni e modelli che presentino anche solo delle somiglianze, non è quindi richiesto che il prodotto sia necessariamente un'imitazione pedissequa per determinare l'illiceità del comportamento della controparte, è inoltre possibile cumulare la tutela del disegno e modello con quella del diritto d'autore, ma oltre al carattere creativo sarà necessario dimostrare anche un valore artistico intrinseco del prodotto[100].

La disciplina europea, oltre a tutelare il disegno e modello comunitario registrato (DMC) presso l'EUIPO, offre un'ulteriore possibilità di protezione anche a quei disegni e modelli comunitari che non risultano registrati. Le principali differenze di questa forma di tutela riguardano il periodo di protezione, ridotto a tre anni per i disegni e modelli non registrati dalla data di divulgazione al pubblico, con prolungazione non effettuabile e con un'ulteriore limitazione del raggio di tutela solo alle copie pedisseque[101].

---

[99] Si veda F. SANNA in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 372. Il disegno o modello registrato presso l'UIBM può accedere alla registrazione comunitaria presso l'Ufficio europeo di Alicante, questo entro 6 mesi dalla presentazione della domanda nazionale. I disegni e modelli comunitari sono disciplinati dal regolamento CE 12 dicembre 2001 n.6/2002, con un'unica registrazione si può quindi ottenere una protezione estesa in tutto il territorio della UE. In tal senso si veda G. GHIDINI, G. CAVANI, (nt. 27), 62. Per ciò che concerne il deposito multiplo si veda anche l'art. 39 c.p.i., dove si disciplina che: "Con una sola domanda può essere chiesta la registrazione per più disegni e modelli purché destinati ad essere attuati o incorporati in oggetti inseriti nella medesima classe della classificazione internazionale dei disegni e modelli".

[100] Come stabilito dall'art. 41 c.p.i., si veda anche F. SANNA in P. MARCHETTI, L. C. UBERTAZZI, (nt. 10), 367. Si riconosce al titolare del disegno e modello il diritto esclusivo di utilizzarlo in qualunque modo o forma, vietando a terzi soggetti ogni uso non autorizzato. La disciplina sul contenuto dell'esclusiva dell'istituto esprime i propri principi generali in materia di contenuto del diritto esclusivo. La possibile cumulazione della tutela del disegno e modello con il diritto d'autore si indica anche nella sentenza della CGCE, sez. III, 12 settembre 2019, n. 683, in *Dirittoegiustizia.it*.

[101] In tal senso si veda il regolamento n. 6/02/CE e A. VANZETTI, V. DI CATALDO, (nt. 48), 528.

2.4. I diritti d'autore

Il diritto d'autore è un istituto giuridico che tutela le creazioni intellettuali frutto delle opere di ingegno, con utilizzi sia in campo letterario che artistico. Il diritto d'autore è stato disciplinato in Italia per la prima volta dalla legge 633/1941 (da ora la legge o l. aut.), e come stabilito dall'art. 1 l. aut., protegge gli autori di "*opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione*" verso utilizzi impropri dell'opera, garantendo all'autore una serie di diritti di natura sia economica che morale. L'art. 2 l. aut. dispone che sono tutelabili come diritto d'autore tutte le opere letterarie, drammatiche, scientifiche, didattiche, religiose, in forma scritta o orale, le opere di composizione musicale, opere drammatico-musicale, variazioni musicali, opere coreografiche come pantomimiche, i disegni e le opere di architettura, le opere dell'arte cinematografica o fotografica, i programmi per elaboratore e le banche dati[102].

Oltre al diritto d'autore sono tutelati diritti definiti come connessi, che hanno lo scopo di ricompensare lo sforzo intellettuale e creativo e gli investimenti di coloro che permettono al pubblico di fruire delle opere citate all'art. 2 l. aut.. La legge sancisce che questi soggetti sono ad esempio gli artisti interpreti ed esecutori musicali ed audiovisivi, i produttori discografici, le emittenti radiofoniche e televisive. I creatori di opere tutelabili dal diritto d'autore possono essere proprietari di diritti sia di carattere esclusivo, sia legati al compenso derivante di natura economica. I diritti con carattere di esclusività permettono di concedere o meno l'autorizzazione all'utilizzo dell'opera soggetta a protezione: il titolare del *copyright*[103] può infatti vantare una serie di diritti patrimoniali, come il diritto di riproduzione, il diritto di trascrizione dell'opera, il diritto di esecuzione, recitazione o rappresentazione in pubblico,

---

[102] Nella normativa italiana non è presente una definizione di opera dell'ingegno, le creazioni citate nell'art. 1 della legge rivestono un carattere prettamente esemplificativo, si veda in tal senso T. ASCARELLI, *Teoria della concorrenza e dei beni immateriali*, Giuffrè, Milano, 1960, 698. Risulta dunque di fondamentale importanza l'art. 2 l. aut., in quanto tale fornisce una chiarificazione sul significato e la portata della nozione generale di creazione, come illustrato da P. AUTERI, (nt. 34), 492.

[103] Con *copyright* si designa una riserva del diritto d'autore, che viene esplicitamente dichiarata dall'editore o dall'autore stesso, anche con la semplice apposizione del caratteristico simbolo © in ogni sua pubblicazione, per evitare riproduzioni non autorizzate dell'opera. Nell'*IPTK Basics* dell'EUIPO, (nt. 93), 84, si descrive l'esistenza di due tradizionali e filoni principali per ciò che concerne il diritto d'autore: quello di origine anglosassone, nel Regno Unito, nelle sue ex colonie (Australia, Sudafrica, Nuova Zelanda e India), in Irlanda e negli Stati Uniti d'America (USA) che applicano il sistema del *copyright*, e quello di origine dell'Europa continentale, con i principi del *droit d'auteur*. Alcuni paesi africani hanno assorbito il sistema francese, anche i paesi dell'America centrale e meridionale applicano il sistema del *droit d'auteur*. I due sistemi differiscono sotto alcuni aspetti essenziali, compresa l'attribuzione del ruolo dell'autore e il tipo di diritti conferiti. Si veda anche G. GHIDINI, G. CAVANI, (nt. 27), 159.

diritto di comunicazione e distribuzione, d'elaborazione, traduzione e pubblicazione, ha inoltre la facoltà di noleggiare l'opera e di darla in prestito. Il titolare dell'opera ha invece il diritto morale di rivendicare la paternità di questa, con la possibilità di ritirarla dal commercio e pubblicarla o mantenerla inedita. Come disciplinato dagli artt. 12-19 l. aut. i diritti al compenso sono diversamente legati alla sfera economica, permettono di acquisire e tutelare i guadagni legati alla diffusione dell'opera verso quei soggetti che hanno partecipato al processo creativo. Il diritto all'utilizzo dei proventi economici derivati dall'opera perdurano per tutta la vita dell'autore e sino a settant'anni dopo la sua morte come stabilito dall'art. 25 l. aut., mentre non è posto nessun limite alla durata del diritto morale. Una volta terminato il periodo di tutela previsto dall'ordinamento, l'opera diventerà di dominio pubblico e potrà essere utilizzata da chiunque, sempre rispettandone l'onore e la personalità dell'autore dell'opera originale[104].

Nel già illustrato art. 1 l. aut. si stabilisce che le opere tutelabili come diritto d'autore devono presentare un "*carattere creativo*". All'art. 6 l. aut. si aggiunge che: "*Il titolo originario dell'acquisto del diritto di autore è costituito dalla creazione dell'opera, quale particolare espressione del lavoro intellettuale*". La legge richiede quindi il requisito del carattere creativo dell'opera come risultato di un'attività dell'ingegno umano; sebbene la dottrina e la giurisprudenza non definiscano in maniera omogenea cosa s'intende per carattere creativo, o stesso viene generalmente ricollegato a concetti quali la novità e l'originalità[105].

Tradizionalmente però la dottrina differenzia il requisito dell'originalità da quello della novità. Per originalità s'intende un "*risultato di un'attività dell'ingegno umano*" che non

---

[104] Parte della dottrina considera il diritto d'autore come un diritto unitario, costituito sia da facoltà patrimoniali che personali, strettamente connesse fra loro: è la teoria della c.d. monistica, si veda in tal senso E.P. CASELLI, *Codice del diritto d'autore*, Utet Giuridica, Torino, 1943, 325. Tuttavia un'altra parte della dottrina sostiene che sia il diritto patrimoniale che quello morale hanno finalità e contenuti diversi, sebbene sorti a titolo originario in capo allo stesso soggetto. Si esprime in tal senso P. AUTERI, (nt. 102), 525.

[105] In tal senso si veda la sentenza della Cass., sez. I, 12 marzo 2004, n. 5089, in *Pluris*, in cui si evidenzia che: "In tema di diritto d'autore, il concetto giuridico di creatività, cui fa riferimento la norma ex art. 1 della legge n. 633 del 1941, non coincide con quello di creazione, originalità e novità assoluta, riferendosi, per converso, alla personale e individuale espressione di un'oggettività appartenente alle categorie elencate, in via esemplificativa, nell'art. 1 l. aut., di modo che un'opera dell'ingegno riceva protezione a condizione che sia riscontrabile in essa un atto creativo, seppur minimo, suscettibile di manifestazione nel mondo esteriore, con la conseguenza che la creatività non può essere esclusa soltanto perché l'opera consiste in idee e nozioni semplici, ricomprese nel patrimonio intellettuale di persone aventi esperienza nella materia". Perciò, il concetto giuridico di creatività citato nel art. 1 l. aut., non coincide con quello di creazione, di originalità e di novità assoluta, ma si riferisce alla personale e individuale espressione di oggettività delle categorie elencate e alla capacità di manifestare nel mondo esteriore un atto creativo. L'opera deve perciò possedere certe caratteristiche derivanti dal personale contributo posto dal suo autore, mentre non influisce il suo intrinseco valore artistico. Sono quindi privi di protezione prodotti senza autonomo carattere distintivo, come brevi slogan, frasi, formule matematiche. Si veda in tal senso G. GHIDINI, G. CAVANI, (nt. 27), 165.

presenti elementi banali, ma che sia invece una rivelazione della personalità dell'autore, mentre per novità viene intesa la presenza di "*elementi essenziali e caratterizzanti*"*;* la tutela potrà essere perciò applicata a sole opere nuove che presentino caratteri di differenziazione rispetto le opere preesistenti[106]. La legge non prevede ulteriori requisiti quali la liceità, il valore artistico o il merito, in quanto questi risultato elementi di carattere soggettivo, che possono mutare e variare nel tempo.

L'ordinamento all'art. 70 l. aut. prevede delle eccezioni al diritto d'autore, è infatti possibile la libera utilizzazione dell'opera nell'ambito dell'insegnamento o della ricerca, come avviene nel caso di riassunti, citazioni o riproduzione di brani o parti di esse per la comunicazione a studenti o per finalità illustrative non di carattere commerciale. E' possibile anche la pubblicazione attraverso internet a titolo gratuito di immagini che però presentino una bassa risoluzione o siano degradate, sempre per usi che non siano a scopro di lucro ma per fini didattici o letterari[107].

Per quanto concerne il deposito, l'art. 6 l. aut. stabilisce che i diritti legati all'opera si costituiscono con la creazione dell'opera stessa, quale espressione del lavoro intellettuale, non è quindi necessario un deposito o di una particolare registrazione per far valere i diritti sopra elencati, i quali hanno una funzione amministrativa di pubblicità notizia[108]. Il deposito avviene presso il Registro Pubblico Generale delle Opere Protette. In tema di registrazione è poi importante citare la Società Italiana Autori ed Editori (SIAE), che si occupa della tenuta del Registro pubblico per i programmi software e consente di rendere pubblica l'esistenza e la titolarità dei diritti ad essi collegati.

---

[106] Si veda P. AUTERI, (nt. 34), 200. Il giudice dovrà dunque valutare la presenza dei requisiti richiesti, sia sotto il profilo della compiutezza espressiva, sia sul profilo della novità. Poi dovrà valutare se l'opera costituisce plagio, in tal senso si veda anche la Cass., sez. I, 23 novembre 2005, n. 24594, in *Pluris*, dove si è valutato che: "Il carattere creativo e la novità dell'opera (nella specie, opera musicale) sono elementi costitutivi del diritto di autore sull'opera stessa, con la conseguenza che, in caso di verifica se tra due opere o parti di opera sussiste plagio, occorre preliminarmente accertare se l'opera o parte dell'opera che si pretende plagiata abbia i requisiti per beneficiare della protezione richiesta sia sotto il profilo della compiutezza espressiva della sua attitudine ad essere considerata autonomo apporto creativo sia sotto il profilo della novità".

[107] Si veda in tal senso F. SANNA in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 1690, secondo dottrina e giurisprudenza in parte maggioritaria la disposizione ha un carattere eccezionale e va interpretata comunque restrittivamente. Sono previsti quindi dei limiti alla facoltà di citazione, come per finalità di critica, discussione, insegnamento o ricerca scientifica.

[108] In tal senso si veda Cass., sez. I, 04 febbraio 2016, n.2197, in *Pluris*, dove si indica che l'art. 11 l. aut. va interpretata nel senso che: "L'equiparazione degli enti committenti agli autori dell'opera non deroga al principio fondamentale dell'art. 6 della stessa legge, laddove stabilisce che il titolo originario dell'acquisto del diritto di autore è costituito dalla creazione dell'opera, quale particolare espressione del lavoro intellettuale. Pertanto, quale che sia il rapporto dell'ente con la persona fisica al cui ingegno l'opera si deve, è l'atto creativo che attribuisce in via originaria la paternità dell'opera".

2.5. Cumulazione e integrazione dei diritti di proprietà

Analizzando singolarmente ogni istituto giuridico e valutandone la disciplina di tutela si è potuto notare come questi sistemi di protezioni previsti dal legislatore siano sensibilmente diversi, pur ravvisandosi una *ratio* comune.

Proprio per questo motivo è risultato fondamentale valutare ogni singolo caso, definendone le caratteristiche principali, in quanto ci permette di avere una visione più generale di quelli che sono gli strumenti di protezione del know-how delle imprese. Lo stesso know-how è una definizione, che a mio avviso, risulta molto generalista e può comprendere conoscenze ed informazioni che presentano connotazioni notevolmente diverse, ciò comporta la necessità di definire con precisione quali siano gli strumenti di tutela giuridica più adeguati a seconda dell'occorrenza dell'impresa, delle tempistiche che si voglio adottare, dei costi da sostenere e in particolare delle caratteristiche intrinseche dell'oggetto di tutela. Inoltre anche la tipologia d'impresa risulta una variabile non di secondaria importanza, che va presa sempre in considerazione: si analizzerà nello specifico il caso delle imprese digitali e dei strumenti di tutela applicabili al loro capitale immateriale, il quale necessita di particolari forme di protezione vista la particolare natura e l'elevato know-how in esso contenuto.

I diversi istituti giuridici di tutela della proprietà intellettuale e industriale non rappresentano tuttavia forme distinte e indipendenti di protezione, poiché a seconda del caso concreto, possono essere integrate e cumulate tra loro al fine di offrire una protezione più completa del know-how. Proprio le discipline del c.p.i., del c.c. e della legge sul diritto d'autore offrono all'imprenditore la possibilità di valutare possibili cumuli e integrazioni delle tutele, ampliando e rafforzando la difesa del capitale dell'impresa, sia a livello applicativo che a livello temporale[109].

---

[109] Si veda la tabella A in appendice in cui sono indicati i principali sistemi di protezione delle innovazioni di prodotto o di processo delle imprese in UE. Si veda anche l'art 17 della direttiva europea 1998/71 e l'art. 44 c.p.i., che prevedono il cumulo delle tutele tra disegno e modello e diritto d'autore nel diritto europeo, qualora soddisfino i requisiti richiesti, stabilendo che: "I disegni o modelli registrati in uno Stato membro o con effetti in uno Stato membro a norma della direttiva sono ammessi a beneficiare altresì della protezione della legge sul diritto d'autore vigente in tale Stato fin dal momento in cui il disegno o modello è stato creato o stabilito in una qualsiasi forma", si veda in tal senso G. GHIDINI, G. CAVANI, (nt. 27), 64. In dottrina si presentano numerosi casi di cumulo delle discipline, si veda ad esempio A. OTTOLIA, (nt. 23), 1115, in cui trattando l'allineamento dei termini di prescrizione, prevede una possibilità di cumulazione dell'azione extracontrattuale con quella contrattuale, o ancora per le violazioni delle condizioni di utilizzo di informazioni segrete già legittimamente acquisite *ex contractu* e degli obblighi di fedeltà del dipendente art. 2105 c.c. Un altro caso di cumulo di tutela si evidenzia tra l'azione di concorrenza sleale con quella contrattuale che si verifichi, ad esempio, nel caso in cui l'impresa concorrente si approfitta dell'inadempimento contrattuale altrui. In particolare, nel segreto commerciale gli aspetti contrattuali ed extracontrattuali sono strettamente connessi, più che in ogni altro settore del diritto della proprietà intellettuale e della concorrenza, come rilevato da C. GALLI, *Potenziale perpetuità della tutela del know-how e contrattualizzazione degli impegni di riservatezza,* in *Dir. ind.*, 2018, II, 113.

Si pensi ad esigenze di natura prettamente temporale, come può avvenire durante le prime fasi di sviluppo del know-how, data l'urgenza iniziale si potrebbe preferire l'applicazione di istituti di facile e veloce attuazione; solo successivamente avverrebbe un adeguamento con altre forme di protezione più strutturate, una volta che la proprietà è in grado di rispondere a tutti quelli che sono i requisiti e le disposizioni richiesti dall'ordinamento giuridico, disposizioni che possono richiedere un certo *iter* o tempistiche più lunghe[110]. Senza un'integrazione iniziale con altre forme di tutela, il know-how sarebbe liberamente esposto al mercato e non presenterebbe adeguate difese contro comportamenti anticoncorrenziali di soggetti esterni, l'impresa vedrebbe così annullato il valore e il vantaggio competitivo derivato dal know-how.

Oltre a questi motivi di carattere prettamente organizzativo-temporale della tutela, pensiamo al cumulo come all'opportunità di applicare diverse discipline a livello processuale. Il convenuto, che subisce un illecito da un terzo soggetto, può così rivendicare l'applicazione di più normative o la possibilità di intraprendere strade diverse per la difesa dei propri diritti di proprietà; ad esempio il soggetto possessore di un segreto commerciale può valutare, per rivendicare i propri diritti, l'applicazione delle norme civili o di quelle previste dal codice penale, a seconda della fattispecie. La possibilità di applicare norme di diversa natura da parte del giudice amplierà il campo di tutela del know-how, scoraggiando maggiormente quelli che sono possibili atti illeciti da parte di terzi soggetti.

La stessa natura dell'informazione, del capitale intellettuale o industriale dell'impresa può modificarsi nel tempo, e può quindi richiedere l'applicazione di istituti diversi, anche a seconda delle esigenze del mercato, mutando nel corso degli anni. Pensiamo alla necessità di garantire una maggiore tutela alle informazioni in possesso all'impresa, in particolare se le stesse, come spesso succede, cambiano nel tempo e acquisiscono maggior valore necessitando, quindi, di essere protette con strumenti più specifici.

Si pensi infine alle necessità di tutela a livello territoriale: in un mondo sempre più globalizzato è essenziale offrire alle imprese strumenti che diano una protezione completa a livello mondiale, mentre certi istituti giuridici, vincolati da principi di territorialità, prevedono una mancanza di regolamentazione al di fuori del territorio di applicazione, provocando forti minacce alle imprese che potrebbero così subire comportamenti illeciti da soggetti esterni che

[110] Si pensi all'*iter* di domanda di registrazione di un brevetto.

operano a livello extraterritoriale, non vincolati dalle discipline sulla tutela della proprietà in quanto operanti in mercati dove l'acquisizione illecita del know-how*,* o di quel specifico istituto giuridico, non viene adeguatamente regolamentato, generando così ampi "spazi bui" per lo sviluppo di quelli che sono comportamenti anticoncorrenziali, provocando vantaggi competitivi di natura prettamente illecita, senza lasciare alle imprese una vera ed efficiente possibilità di difendersi[111].

2.5.1. Le relazioni tra segreti commerciali e i brevetti

Abbiamo già visto come la regolamentazione italiana ed europea in materia di proprietà industriale e intellettuale permetta all'imprenditore, di fronte ad un'invenzione, di poter scegliere tra diverse tipologie di tutela, confrontando nello specifico i benefici ottenibili da un segreto commerciale e da un brevetto si evidenzia che un istituto giuridico può risultare più adeguato rispetto l'altro a seconda delle caratteristiche dell'invenzione, del settore industriale e delle necessità dell'imprenditore. Vi è, ad esempio, maggiore propensione alla tutela come segreto commerciale rispetto al brevetto nei settori in cui le innovazioni si succedono in maniera rapida, come nel settore delle gare automobilistiche o nel motociclismo. In questi settori il mantenimento della segretezza delle invenzioni risulta di fondamentale importanza, tuttavia la segretezza non è conciliabile con la disciplina prevista dal brevetto, giacché richiede la pubblicazione dell'invenzione, la quale comporterebbe un indubbio vantaggio ai *competitors*[112]*.* Tuttavia*,* come indicato dai dati nella tabella B e i grafici C in appendice, sia le PMI che le grandi imprese della zona UE utilizzano maggiormente segreti commerciali rispetto ai brevetti, con risultati divergenti tra Stati membri[113].

Anche se ambedue le tutele possono venir riconosciute a livello europeo e sono regolate dal Codice della Proprietà Industriale, il loro oggetto risulta notevolmente diverso: come abbiamo

---

[111] Si pensi ai modelli d'utilità che, come indicato dal documento *IPTK basics* dell'EUIPO (nt. 93), 64, rappresentano un diritto di natura territoriale, il quale offre protezione esclusivamente nel paese dell'autorità emittente. Si veda anche la tabella A in appendice, da cui risulta che i diritti di proprietà intellettuale non sono tra i sistemi più utilizzati dalle imprese per la tutela delle innovazioni.

[112] Si veda l'articolo di C. MORBIDI, *I rapporti tra know-how e brevetto,* Brevettinews, 2018 e C. GALLI, (nt. 109), 115. La *ratio* della funzione brevettuale può infatti considerarsi opposta a quella del segreto: nel brevetto si applica la teoria del c.d. "contratto sociale", per cui la collettività remunera l'acquisizione dell'invenzione al patrimonio pubblico contraccambiando attraverso l'attribuzione di diritti esclusivi di uso dell'invenzione, benché limitato nel tempo. Ciò non è ovviamente presente nella disciplina dei segreti commerciali.

[113] Come indicato nel report dell'EUIPO, *Protecting innovation through trade secrets and patents: determinants for European Union firms*, 2017, reperibile in internet al seguente indirizzo: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf.

già illustrato mentre per i brevetti l'invenzione deve presentare una natura prettamente tecnica, con caratteristiche nuove, originali, applicabili a livello industriale e lecite, e richiede un esame complesso da parte dell'ente preposto alla brevettazione, il segreto commerciale non impone invece limiti restrittivi particolari all'oggetto di tutela, applicandosi ad ogni forma di informazione, anche di carattere non prettamente tecnico, ma con requisiti che rispondano sempre agli elementi presentati all'art. 98 del c.p.i.[114]

Ulteriore differenza riguarda l'ambito di tutela, il brevetto garantisce all'inventore o al suo avente causa, il monopolio legale esclusivo ed escludente sull'utilizzo commerciale di un'invenzione, configurandosi come un diritto assoluto ma limitato sia nel tempo (vent'anni) che nello spazio. Differentemente la disciplina dei segreti commerciali è relativa e invocabile solo nei confronti di terzi che abbiano acquisito, rivelato o utilizzato in modo illecito le informazioni protette; la tutela garantita risulta quindi più aleatoria ma potenzialmente illimitata sia sul profilo temporale che sul piano territoriale, rappresentando perciò un'ottima alternativa al regime brevettuale[115].

Anche i costi da sostenere per poter godere delle due tutele possono differire fortemente, in particolare il brevetto risulta sicuramente più costoso, sia per le risorse necessarie per la presentazione della domanda di brevetto, che per il mantenimento del brevetto stesso una volta concesso, il quale richiede il pagamento di cospicue tasse annuali da parte del detentore. Nel segreto commerciale i costi dipendono in particolare dalla natura dell'oggetto tutelato, dell'uso che si fa dell'informazione e da quante persone sono a conoscenza del segreto, ma la procedura risulta sicuramente più semplificata e il mantenimento del segreto meno costoso rispetto all'*iter* brevettuale[116].

---

[114] Tuttavia si evidenzia che le informazioni tutelabili come segreti commerciali possono presentare un carattere meramente commerciale (come le strategie di marketing, le liste clienti profilate etc.), oppure un carattere più innovativo, legate anche all'esperienza tecnica. Il riconoscimento alla tutela esclusiva trova la propria *ratio* nell'incentivare l'innovazione e gli investimenti in attività di ricerca e sviluppo. Questi settori sono caratterizzati infatti da un'elevata obsolescenza, ciò non renderebbe giustificato per l'impresa investimenti di tempi e costi per la conclusione delle procedure di rilascio di un brevetto, come sostenuto da S. SERAFINI, (nt. 20), 1330.

[115] Si veda C. GALLI, (nt. 109), 116. e M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 40, le antinomie tra segreto e brevetto non si fermano alla sola tematica della segretezza e alla pubblicazione, ma bensì più importanti elementi di differenziazione sono rilevati nella durata delle rispettive protezioni e nell'assenza dei limiti territoriali che sono disposti dalla disciplina del segreto. Il segreto commerciale, nel caso le informazioni riservate presentino tutti i requisiti di brevettabilità, può considerarsi un'ottima alternativa al brevetto, in quanto risulta essere una protezione potenzialmente perpetua.

[116] Se l'impresa non ha le capacità economiche per sostenere *l'iter* di brevettazione o l'informazione non presenta tutti i requisiti di brevettabilità, il segreto commerciale risulta dunque l'unica forma disponibile per garantire la tutela dell'invenzione, come sostento da C. GALLI, (nt. 109), 117.

In aggiunta alle differenze fin qui illustrate, si rileva una staticità del brevetto nel tempo, contrariamente al segreto commerciale e al know-how a esso connesso, che presenta invece una certa dinamicità. Possiamo appunto definire che il brevetto recepisce un determinato stadio dell'innovazione della tecnica, con necessaria descrizione pena la nullità, come stabilito dall'art. 51 c.p.i., rivendicando nella sua pubblicazione tutti gli aspetti che ne caratterizzano l'invenzione. Differentemente, il segreto può fungere da mutevole e continuativo progresso, non vincolato da particolari formalizzazioni, l'individuazione del know-how a esso configurato potrà così arricchirsi in momenti successivi di ulteriori dettagli e aspetti. Perciò, descrivendo la situazione tramite una metafora, possiamo presentare il brevetto come una fotografia dell'innovazione, in grado di definire la situazione in un preciso istante con un immagine che risulti più nitida e riproducibile al pubblico possibile, il segreto potrà venir invece rappresentata come una serie di fotogrammi, capace di una maggiore dinamicità e possibilità di modifica nel corso degli anni[117].

La valutazione che dev'essere effettuata dall'imprenditore per decidere quale protezione sia maggiormente adeguata al proprio capitale non va effettuata prendendo in considerazione il brevetto o il segreto commerciale in maniera isolata e separata, in modo tale che l'applicazione di un istituto escluda l'altro; le due tutele possono essere cumulate, sfruttando appieno le loro caratteristiche. Visti gli elementi presentati finora possiamo dire che i segreti commerciali sono più adeguati per la tutela di procedimenti piuttosto che per i prodotti, essendo i primi più difficilmente decompilabili, oppure un utilizzo ottimale dei due istituti può essere effettuato ad esempio in maniera complementare proteggendo l'invenzione, in quanto tale, con il brevetto, mentre il know-how di corredo tramite la protezione delle informazioni segrete, si otterrà così una tutela più ampia e sicura[118].

---

[117] Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 40 ss. e S. SERAFINI, (nt. 20), 1336, i due strumenti rispondono con caratteristiche diverse alle soluzioni trovate, e quindi a distinti interessi degli inventori: salvo casi del tutto eccezionali, come ad esempio la ricetta della Coca-Cola, ove il trovato ha una sostanziale descrittività ed è suscettibile di uno sfruttamento economico durevole, l'impresa avrà interesse alla brevettazione dell'invenzione; diversamente, nel caso di miglioramenti che si inseriscono in un flusso innovativo costante, e che quindi sono destinati ad avere una breve durata, sarà, secondo l'autore, più congeniale il regime del segreto. Questo in conformità alla maggiore capacità di dinamicità del segreto commerciale rispetto al brevetto.

[118] Si veda l'articolo di N. COSA, *Come proteggere le proprie invenzioni: brevetto o segreto industriale?* Iusinrete, 2018 e M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 38, nella domanda di brevetto bisogna escludere dalle rivendicazioni relativi all'invenzioni dati, informazioni e dettagli che rischiano di delimitare l'ambito di tutela del brevetto. Questi possono invece venir mantenuti segreti e in tal modo essere elementi di supporto per l'implementazione di specifiche forme attuative dell'invenzione. Ad esempio, nel settore meccanico, si pensi alla differenza tra i c.d. "disegni d'insieme", che corredano la domanda di brevetto, e i c.d. "disegni operativi", che invece includono determinati particolari del prodotto o del macchinario come dimensioni, tolleranze, materie prime utilizzate ecc.

Ancora la tutela di un'invenzione come segreto può essere adottata in una maniera residuale, quando l'ottenimento di un brevetto non sia possibile o non efficiente/efficace per la mancanza dei requisiti richiesti o per la complessità della domanda di registrazione: questa fase può infatti richiedere un lungo periodo di analisi e sviluppo, anche dai 24 ai 30 a mesi dalla data di deposito della domanda[119]. In via d'urgenza o nelle fasi iniziali l'imprenditore può quindi valutare l'applicazione della tutela dell'informazione come segreto commerciale in funzione accessoria e, solamente in un secondo momento, avviare l'*iter* di brevettazione.

Infine si consideri il periodo che intercorre tra il deposito del brevetto e la sua pubblicazione, dove viene a configurarsi una sorta di regime "ibrido" tra i due istituti: il brevetto risulta infatti ancora in uno stato di domanda ma è potenzialmente già costitutivo di diritto di privativa, in una situazione che potrebbe venir configurata come un limbo, essendo di fatto già un monopolio legale, allegato di documento avente data certa, che verrà però appieno compimento solo con la sua pubblicazione, ma che risulta al contempo non accessibile ai terzi, in quanto non essendo ancora rivelato al pubblico, le proprie informazioni risultano segrete all'esterno. Dunque, in questa fase ibrida, si realizzano i vantaggi sia del brevetto che del segreto, sebbene per un periodo limitato di tempo; il periodo di segretezza del brevetto terminerà con la pubblicazione, comportandone la conoscenza al pubblico dominio[120].

2.5.2. Il caso dei software

Analizziamo ora un caso specifico, ossia i sistemi di tutela previsti per i software*,* tale tecnologia ha, negli ultimi anni, raggiunto un'importanza sempre maggiore, parallelamente a questa crescita anche la disciplina in materia di tutela ha visto modificarsi notevolmente, sono state infatti introdotte nuove regolamentazioni attraverso un'integrazione degli istituti del segreto commerciale, del brevetto e del diritto d'autore[121].

Per software intendiamo tutti i componenti modificabili di un sistema o di un apparecchio e,

---

[119] I dati per il procedimento di esame e concessione di un brevetto sono stati estrapolati dal sito ufficiale del Ministero dello Sviluppo Economico.

[120] Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 38, C. GALLI, (nt. 109), in dottrina si considera il segreto prodromico e quindi complementare allo stesso processo di brevettazione. Questo perché se l'invenzione è divulgata prima del deposito non può più essere validamente protetta, non essendo previsti nell'ordinamento italiano o in quello europeo dei "periodi di grazia".

[121] Come evidenziato da E. AREZZO, *Protezione del segreto e tutela del software: convergenze, sovrapposizioni, conflitti*, in *Dir. ind*., 2018, II, 146, il software probabilmente rappresenta l'esempio più emblematico della nuova tendenza che ha visto l'espansione delle forme di tutela per la protezione della proprietà industriale.

più specificamente, in informatica, l'insieme dei programmi che possono essere impiegati su un sistema di elaborazione dei dati. Questi possono essere di sistema, relativi cioè al sistema operativo dell'elaboratore, o di base, ossia l'insieme di programmi e procedure di utilità generale, organizzati in sottoprogrammi o richiamabili dai programmi applicativi, che sviluppano particolari funzioni o costituiti da programmi sviluppati dall'utente[122]. Le invenzioni che possono impiegare un software nell'attuale stato tecnologico fanno parte dei più disparati comparti della tecnica, spaziando dall'informatica alle comunicazioni in generale, o a settori più tradizionali come quelli della meccanica, come nel supporto della medicina. Una sempre maggior importanza stanno guadagnando i software sviluppati per il settore biotecnologico, della genetica, della biologia sintetica; si può dunque sostenere che ormai ogni strumento tecnologico, anche il più semplice, contiene al suo interno un software, più o meno complesso, diventando così un elemento essenziale per lo sviluppo tecnologico[123].
Abbiamo già richiamato l'art. 45, co. 2, c.p.i., dove vengono elencate una serie di creazioni che secondo le disposizioni dell'articolo non possono venir brevettate; tra queste ritroviamo i programmi per elaboratori e quindi i c.d. software. Questa logica ha in realtà un'origine storica ben precisa, infatti queste disposizioni erano già previste nella Convenzione di Monaco del 1973 e già prima dalla legge francese del 1968. Sono diverse le motivazioni che hanno portato a questa scelta: la prima e probabilmente più forte riguarda la scarsa conoscenza del settore della tecnologia all'epoca della Convenzione di Monaco, allora i software erano ancora in fase di sperimentazione e la convinzione diffusa e radicata nelle Istituzioni preposte a regolamentare la disciplina era che esisteva una radicale alterità tra la creazione di un software e i settori tradizionali industriali. Era diffuso inoltre il timore che una tutela brevettuale dei software avrebbe comportato una copertura anche dell'algoritmo alla base del programma, rischiando così di frenare l'innovazione, in aggiunta si temeva che gli Uffici Brevetti non fossero in grado di gestire l'*iter* brevettuale ed il controllo delle procedure

---

122 Si veda Treccani, voce *software,* n.d.

123 A tal proposito si veda E. AREZZO, *Nuove invenzioni e rapporti tra i diversi requisiti di brevettabilità nella giurisprudenza EPO,* in *Dir. ind.*, 2016, II, 159, e E. AREZZO, *Tutela brevettuale e autoriale dei programmi per elaboratore: profili e critica di una dicotomia normativa*, Giuffrè, Milano, 2012, 3 ss. Come indicato dall'EPO è necessario fare una distinzione tra "programma per elaboratore" o software, inteso come istruzioni scritte in linguaggio di programmazione, e invenzione attuata per mezzo di un elaboratore elettronico, queste infatti sono invenzioni le cui rivendicazioni comprendono un elaboratore elettronico o una rete di elaboratori, quindi ogni altra forma di macchina programmabile in cui uno o più elementi caratterizzanti il trovato vengono realizzati attraverso uno o più programmi. Si vedano le linee guida per l'esame sostanziale presso l'EPO (*Guidelines for Substantive Examination in the European Patent Office*), reperibile in internet al seguente indirizzo: http:// www.european-patent-office.org/legal/gui_lines/in- dex.htm.

di domanda di brevettazione di un software, questo per via della novità del settore e della tecnologia, le domande di brevettazione potevano essere inoltre numerose ma con valutazioni più complesse e completamente diverse rispetto ai settori tradizionali. Infine, è importante segnalare anche la posizione dei produttori dei dispositivi hardware, che erano contrari alla possibilità di estendere la tutela del brevetto ai software, in quanto convinti che ciò avrebbe potuto comportare maggiori difficoltà nel commercio dei loro prodotti[124].

La forte crescita degli investimenti nel settore dei software e la difficoltà di applicare tutele efficienti del loro know-how, data la facilità di copiatura dei programmi, hanno aumentato, a partire dagli anni Ottanta del Novecento la richiesta da parte dei *players* del settore di adottare sistemi nazionali di diritti di esclusiva riservati prettamente ai software, che ne erano ancora sprovvisti. Anche la regolamentazione italiana non presentava determinazioni a riguardo, in quanto si applicavano le stesse previsione contenute nella Convenzione di Monaco.

Inizialmente il legislatore comunitario, valutando l'impossibilità di applicare la tutela brevettuale ai software, ha disposto una speciale tutela come diritto d'autore, assimilando il software ad un'opera letteraria[125]. Questa formulazione, ancora oggi vigente, tutela qualsiasi forma di software, sia come codice sorgente che come codice oggetto, non comprende però le idee e i principi alla base del programma, con un'estensione che risulta comunque più limitata rispetto alle regole generali dei diritti d'autore in relazione agli usi leciti concessi ai terzi ma presentando ulteriormente a ciò delle regole di carattere brevettuale, che riservano diritti al datore di lavoro su programmi realizzati da propri dipendenti. La tutela come diritto d'autore ha dimostrato però tutti i suoi limiti nel campo dei software, non riuscendo a garantire un'esclusiva su invenzioni che risolvono un problema tecnico tramite l'utilizzo di elaboratori elettronici e software di tipo applicativo[126].

---

[124] Il processo d'evoluzione della tutela dei software è illustrato da A. VANZETTI, V. DI CATALDO, (nt. 48), 383. Si veda anche G. GHIDINI, G. CAVANI, (nt. 27), 5 ss.

[125] Direttiva CE n.1991/250 recepita in Italia con il d.l. 29 dicembre 1992, n. 518., oggi dir. CE 2009/24 del Parlamento Europeo e del Consiglio del 23 aprile 2009 relativa alla tutela giuridica dei programmi per elaboratore, in *G.U.*, 5 maggio 2009. Come indicato da E. AREZZO, (nt. 121), 146, la direttiva 1991/250 suggellava la scelta dello strumento autoriale come paradigma ufficiale di tutela dei software.

[126] Per codice sorgente s'intende un linguaggio di programmazione in cui vengono scritte e formalizzate un'insieme di istruzioni, tale linguaggio viene poi convertito meccanicamente in un codice binario che costituisce il codice oggetto. In tal senso si veda l'articolo di A. JEDRUSIK, *Patent protection for software-implemented inventions,* in WIPO Magazine, 2017, in cui si sostiene che il ricorso al diritto d'autore come unico sistema di protezione protegge solamente dalla copiatura letterale del codice sorgente o dell'oggetto, mentre non protegge l'invenzione sottostante implementata dal software. Ulteriore critica è mossa da E. AREZZO, (nt. 121), 148, in quanto l'atto del funzionamento del programma, inteso come la funzionalità che consente di svolgere, che rappresenta la parte "più preziosa" del software, non sarebbe tutelata dal paradigma autoriale.

Al contempo il sistema di tutela del diritto d'autore, rispetto al brevetto, presenta importanti vantaggi per le imprese dal lato dell'immediatezza della protezione, in quanto non è necessario ottemperare a nessuna formalità, né è necessario attendere una valutazione positiva da parte di un ufficio competente, come invece avviene per il brevetto; inoltre la tutela è decisamente meno onerosa e ha un estensione temporale più lunga[127].

Dagli anni 90' in poi sia l'EPO che le giurisprudenze nazionali hanno ristretto il divieto di brevettazione dei software ai soli "processi" che risultano privi di applicazione pratica. Se l'invenzione attuata tramite un elaborato è in grado invece di produrre un "effetto tecnico" la brevettabilità del software è stata ammessa, secondo la teoria del c.d. "carattere tecnico" un'elaboratore diviene brevettabile se l'invenzione descritta e rivendicata presenta capacità di realizzare concrete applicazioni pratiche, che si esternano attraverso l'impiego o la direzione di strumenti tecnici[128]. Attualmente sia l'EPO che gli Uffici nazionali continuano ad applicare questa concezione, considerando brevettabili le invenzioni di software, sia nel caso che l'effetto realizzato dal software sia interno al computer[129], sia se si realizza esternamente, come nel caso di gestione e governo di un procedimento industriale[130]. Tuttavia il processo giurisprudenziale che ha portato all'accettazione della tutela brevettuale non è stato agevole, questo dovuto principalmente alla natura stessa del software, definita come "tecnologia

---

[127] Come indicato anche da E. AREZZO, (nt. 121), 149, il diritto d'autore presenta infatti, rispetto al brevetto, indubbi vantaggi per le imprese. Questo non solo in termini di immediatezza della protezione, in quanto non è necessario ottemperare ad alcuna formalità di sorta, né attendere il vaglio positivo di alcun ufficio, ma anche perché si riscontrano vantaggi in termini di gratuità della tutela e di estensione temporale della protezione.

[128] La teoria del "carattere tecnico" è presentata da G. GHIDINI, G. CAVANI, (nt. 27), 7. La scelta del legislatore fu probabilmente spinta principalmente da motivi di carattere politico-economico, piuttosto che da motivazioni di pura logica giuridica. Anche E. AREZZO, (nt. 121), 149, sottolinea come già prima dell'adozione della direttiva CE 1991/250, l'EPO iniziava a rilasciare brevetti concernenti invenzioni che rivendicavano in una qualche misura l'utilizzo di un software al loro interno. Questo a condizione che i software producessero un risultato tecnico che andasse oltre la mera interazione funzionale fra mezzi tecnici, ossia l'hardware e il software.

[129] Come ad esempio software che organizzino memorie del computer o rielaborazioni dell'immagine sullo schermo del sistema, o anche software che migliorino il funzionamento di unità di memoria volatili dell'elaboratore facilitandone il trasporto di dati contenuti in un file.

[130] Possono venir considerate tali applicazioni dell'informatica per la soluzione di problemi tecnici esterni al computer, come software che gestiscono un'apparecchiatura di radiografia per migliorare l'esposizione dei pazienti ai raggi X, oppure software che controllino il sistema di frenatura di un veicolo. Un appello dell'IBM (causa numero T. 1173/97) dinanzi alla Commissione Tecniche di Ricorso dell'EPO ha fornito utili indicazioni a riguardo la mancanza di brevettabilità dei software. Il Consiglio ha affermato, in una lettura degli articoli pertinenti alla materia, che questi non comportavano che tutti i programmi per elaboratore erano esclusi dalla brevettabilità, per conformarsi così all'art. 27 dell'accordo TRIPS, in quanto, in tale articolo, per programmi per computer ci si riferiva solo a quelli di carattere non tecnico. In altre parole, fintanto che un programma per computer è tecnico, il supporto in cui è registrato è irrilevante ed è, di fatto, brevettabile. Si veda in tal senso A. JEDRUSIK, (nt. 126). E. AREZZO, (nt. 121), 149, aggiungendo che, sebbene ad oggi la possibilità di far ricorso allo strumento brevettuale non sia mai stata ufficialmente sancita, né a livello nazionale né europeo, la prassi dell'EPO si è più che consolidata nell'applicare la teoria del carattere tecnico sopra esposto.

dell'informazione" o "*information technologies*", questo settore rientra appieno nella nuova categoria di invenzioni che le Commissioni Tecniche di Ricorso ha definito come "*mixed type of claims inventions*", cioè presentanti caratteristiche sia tecniche che non tecniche, trovati che, ad un primo sguardo, apparirebbero non tutelabili come brevetto, in quanto contenenti elementi tra quelli definiti nel co. 2 dell'art. 52 del CBE[131].

Ancora oggi rimane comunque difficile l'interpretazione della valutazione dell'effetto tecnico stabilito dall'EPO come requisito necessario per la brevettazione; risulta infatti non facile la determinazione della linea di confine tra software dotati di effetti tecnici e software che invece ne sono privi, tant'è che la Commissione Europea ha cercato più volte di emanare una direttiva in materia per ridurre le incertezze, ma ad oggi il problema non è stato ancora risolto.

Se invece guardiamo alla disciplina statunitense, questa sembra prevedere una maggiore apertura per ciò che concerne la tutela dei software come brevetti, probabilmente il peso economico notevole del settore in USA ha richiesto la necessità di stabilire un negozio giuridico di tutela dei software adeguato ed efficiente qual è il brevetto[132].

L'introduzione della direttiva CEE 1991/250 relativa alla tutela giuridica dei programmi è stata emanata con l'obiettivo di sviluppare ulteriormente la tecnologia all'interno della UE, promuovendo la libera circolazione e l'appropriabilità delle idee e degli algoritmi sottesi ad ogni programma[133]. Si sono previste due eccezioni che escludono e limitano l'applicazione del diritto d'autore: la "*black box analysis*", che consente all'acquirente del programma di osservare, studiare e sperimentare il funzionamento del programma nel momento in cui

---

131 Per CBE s'intende la Convenzione sulla concessione di brevetti europei (CBE, Convenzione sul brevetto europeo) del 5 ottobre 1973, da ultimo modificata conformemente all'atto di revisione adottato dalla Conferenza OEB il 29 novembre 2000 (CBE 2000). L'espressione "*mixed type of claims inventions"* è stata per la prima volta citata nelle decisioni Comvik/Two identities, T. 0641/00, 26 settembre 2002, e Game machine/ GAMEACCOUNT, T. 1543/06, 29 giugno 2007, in E. AREZZO, (nt. 123), 159. La determinazione dei software come parte del settore della tecnologia dell'informazione è sostenuta da G. GHIDINI, in *Profili evolutivi del diritto industriale*, Giuffrè, Milano, 2015, 197.

132 Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 385. Gli USA hanno una delle industrie a più alta intensità di software al mondo. Solo nel 2014, l'industria dei software ha aggiunto direttamente circa 475,3 miliardi di dollari e indirettamente 1,07 trilioni di dollari, impiegando direttamente 2,5 milioni di persone e sostenendo indirettamente circa 9,8 milioni di posti di lavoro, si veda A. JEDRUSIK, (nt. 126). Negli USA, la protezione brevettuale per le invenzioni relative ai software è limitata a quelle su supporti registrabili, non ai programmi per computer stessi. La giurisprudenza USA non è riuscita a fornire limiti chiari per l'ammissibilità dei brevetti delle invenzioni relative ai software. In tal senso si veda la decisione della Corte Suprema degli USA nel caso Alice Corp. contro CLS Bank Int'l (134 S. Ct. 2347 2014) in A. JEDRUSIK, (nt. 126).

133 Come illustrato da E. AREZZO in *Protezione del segreto e tutela del software: convergenze, sovrapposizioni, conflitti,* Filodiritto, 2017, 1, è necessario il riferimento al co. 2 dell'art. 2 della direttiva CEE 1991/250, dove si limita la tutela solamente a quelle idee o quei principi alla base di qualsiasi elemento di un programma per elaboratore, compresi quelli alla base delle sue interfacce.

vengono effettuate "*operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma*"[134] e la decompilazione, per l'ottenimento di un'interoperabilità fra i diversi software. In nessun caso il legislatore ha però ammesso il ricorso a processi di *reverse engineering*[135].

Nella sentenza SAS Institute Inc. v. World Programming Ltd. la Corte di Giustizia Europea ha delineato limiti ulteriori all'applicazione della disciplina del diritto d'autore nel campo dei software, dichiarando che: "*Il vantaggio principale offerto dal paradigma autoriale come strumento di protezione del software […] risiede nel fatto che esso concerne soltanto l'espressione individuale dell'opera e offre quindi uno spazio sufficiente a permettere ad altri autori di creare programmi simili, o perfino identici, purché si astengano dal copiare*", limitando quindi la tutela del software a quelle copie pedisseque del programma. Oltre a ciò la Corte ha ribadito che la tutela non si applica alla funzionalità generale del software, in quanto questo offrirebbe "*la possibilità di monopolizzare le idee, a scapito del progresso tecnico e dello sviluppo industriale*". Il diritto d'autore proteggerebbe quindi solamente la forma espressiva dell'opera, mentre il suo contenuto e le idee alla base dell'opera stessa non sarebbero tutelate; per aggirare la protezione autoriale di un software basterebbe quindi modificare la forma espressiva, ossia il codice sorgente, così facendo il nuovo programma conseguirebbe il medesimo effetto con una diversa scrittura senza compiere nessun illecito[136].

In contrapposizione a questo, le software *houses,* ossia le imprese specializzate nella produzione di software e applicazioni, hanno potuto godere dell'estensione della protezione

---

134 Si veda l'art. 64-*ter* l. aut. e L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 512, secondo cui si consente solo l'attività di studio che avvengono tramite l'osservazione dall'esterno del programma nel corso del suo funzionamento.

135 Per decompilazione di un software s'intende il processo di traduzione della lingua del programma originale in cui è scritto il software in un codice sorgente che risulta più comprensibile per l'uomo. Si veda l'art 64-*quarter* l. aut. e L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 512, in cui si evidenzia che il divieto di decompilazione del programma si applica laddove da luogo alla predisposizione di copie o di una rielaborazione del software originale. L'unica attività di decompilazione liberalizzata è quella rivolta alla ricerca delle interfacce necessarie a consentirne l'interoperabilità con gli altri software. In aggiunta E. AREZZO, (nt. 133), 3, chiarisce che la direttiva dispone, all'art. 6, che la decompilazione del programma, ossia l'attività che può essere paragonata ai processi già esplicitati di *reverse engineering.* La decompilazione dev'essere effettuata al fine di perseguire l'interoperabilità. Ma se durante queste attività si ottengono delle informazioni segrete, non legate all'interoperabilità tra i programmi o a periferiche esterne, il co. 2 dell'art. 6 della suddetta direttiva stabilisce un divieto assoluto di comunicazione a terzi delle informazioni acquisite con un ulteriore divieto di impiego di siffatte informazioni solo per lo sviluppo, la produzione o la commercializzazione di un software sostanzialmente simile nella sua forma espressiva a quello decompilato dall'utente. Come indicato ulteriormente da L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 512, quindi potranno essere vietate tutte quelle attività di apprendimento effettuate tramite processi di *reverse engineering* che in altri settori sono invece considerate lecite e non scorrette.

136 Si veda in tal senso G. GHIDINI, G. CAVANI, (nt. 27), 8 ss.

come diritto d'autore anche al software in forma di codice oggetto, incomprensibile per l'essere umano[137]; le software *houses* distribuiscono così copie del programma "blindate"[138], mantenendo il codice sorgente rigorosamente segreto, non consentendo la traduzione in un linguaggio comprensibile e non arricchendo la società di nuove conoscenze.

Per concludere, la direttiva consente la tutela del software attraverso il diritto d'autore, accanto alla disciplina prevista per il segreto commerciale, fortificando e rendendo praticamente inespugnabile la tutela: la protezione del codice oggetto permette al proprietario del diritto di distribuire il software al pubblico tutelandolo come diritto d'autore, ma allo stesso tempo riesce a mantenere segrete le componenti più importanti, come il codice sorgente o i concetti, le idee e le procedure alla base della sequenza informatica, rispettando comunque le disposizioni previste per il diritto d'autore, rafforzando la protezione della propria tecnologia con la cumulazione e la sovrapposizione della tutela prevista dagli artt. 98 e 99 c.p.i. come segreto commerciale[139].

---

137 Mentre inizialmente la tutela era prevista solo per software in forma di codice sorgente, unica forma del programma comprensibile per l'uomo.

138 Si veda E. AREZZO, (nt. 133), 5, indicando che la reale finalità della direttiva CE 2009/24 è di proclamare libere dalla tutela, e quindi a disposizione del pubblico dominio, tutti i saperi che ricadono a pieno titolo nella disciplina del segreto commerciale. Un segreto che per di più risulta fortificato e reso inespugnabile dalla protezione prevista anche dal diritto d'autore.

139 A conferma di ciò si veda L. INNOCENTE in P. MARCHETTI, L. C. UBERTAZZI, (nt. 10), 512 e M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 49, dove si sottolinea l'importante normativa a tutela dei software e dei suoi derivati che alcuni esperti sostengono essere addirittura ipertrofica. Il proprietario del programma per elaboratore può infatti ottenete diversi ed efficienti livelli di tutela, con altrettanti penetranti rimedi, il cui cumulo con quelli a tutela pare innegabile. Si veda anche Trib. Torino, sez. spec. propr. industr. ed intell., 16 gennaio 2009, in *Pluris*, in cui il giudice ha ravvisato nella condotta di indebito utilizzo del codice sorgete dell'imputata la fattispecie di cui all'art. 98 c.p.i., oltre che quella prevista dall'art 2598, n.3, c.c.

CAPITOLO 3. GLI STRUMENTI E LE FASI PER LA TUTELA DEL SEGRETO COMMERCIALE

SOMMARIO: 3.1. Premessa - 3.2. Strumenti endoaziendali - 3.2.1. Strumenti endoaziendali verso ex dipendenti - 3.3. Strumenti esoaziendali - 3.3.1. NDA (*Non-disclosure agreement)* - 3.4. *Assessment*, rischi e processi: fasi per la costituzione di un segreto commerciale - 3.5. *Remediation*, misure adeguate - 3.6. Il monitoraggio.

3.1. Premessa

Come illustrato precedentemente, ai sensi del terzo requisito dettato dall'art. 98 c.p.i., per la tutela di un segreto commerciale è necessario che l'imprenditore predisponga delle misure preventive adeguate atte a mantenere la segretezza di certe informazioni aziendali o esperienze tecnico-commerciale[140].

In questo capitolo analizzeremo e presenteremo le modalità e gli strumenti che si possono utilizzare perché ciò venga attuato, verranno inoltre illustrate le fasi di processo necessarie per la costituzione di un segreto commerciale, queste fasi sono fondamentali in quanto permettono la costituzione di una protezione adeguata, predisponendo un segreto in grado di rispondere a tutti i requisiti stabiliti dall'ordinamento giuridico.

L'imprenditore, nel decidere quali misure adottare per tutelare la segretezza delle informazioni, deve prendere in considerazione diversi aspetti, come lo stato dell'arte dell'informazione, gli aspetti essenziali a livello tecnologico, i costi di attuazione e le tipologie di know-how che s'intende proteggere. Sarà dunque necessaria una profonda analisi di questi elementi, in quanto risultano variabili fondamentali per una corretta identificazione delle misure ottimali da predisporre in base al caso specifico preso in esame: la nozione di misure "ragionevolmente adeguate" stabilita dal co. 1, lett. *c*., art. 98 c.p.i, è infatti una nozione relativa e non assoluta, le stesse misure di protezione godono di una certa dinamicità,

---

[140] Art. 98, co. 1, c.p.i., come indicato da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 53 ss. le misure preventive sono elementi costitutivi della disciplina del segreto commerciale. Le misure di protezione devono essere oggettivamente percepibili e verificabili, oltre che adeguate al caso specifico, ossia atte ad esprimere in maniera chiara la volontà di mantenere segrete certe informazioni. A. OTTOLIA, (nt. 23), 1099, interpretando la funzione perseguita dai requisiti del segreto disposti all'art. 98, lett. c*,* c.p.i., riconosce la necessità che si garantisca l'esistenza e il mantenimento dello stato di segretezza secondo una verifica sul possibile piano fattuale. Oltre a ciò, si deve garantire un'indagine piena e strutturata, capace di dimostrare che il titolare dell'informazione ha realmente detenuto e identificato tali conoscenze mediante una verifica, la quale dovrebbe logicamente precedere la comparazione, come disposto dal co. 1 dell'art. 98 c.p.i. Si veda *infra* paragrafo 1.3.1.

essendo oggetto di una costante evoluzione tecnologica e con costi d'attuazione che variano nel corso del tempo[141].

Le misure di protezione saranno applicate secondo un principio di proporzionalità, ciò è stato pienamente riconosciuto anche dalla giurisprudenza delle sezioni dei tribunali specializzate in materia d'impresa. Possiamo sostenere che tale principio deriva, ed è fortemente influenzato, dalla prassi dei paesi di *common law,* se avvicinato ai concetti di diritto civile italiano, può essere declinato in forme come "la normale diligenza", "la prevedibilità secondo le circostanze" o ancora al criterio dello "stato dell'arte"[142].

Le protezioni adottate per mantenere le informazioni segrete avranno una duplice fondamentale funzione: *in primis*, come già evidenziato, sono necessarie per rispondere al terzo requisito stabilito all'art. 98, co. 1, c.p.i., che, se non presente, non consentirebbe di considerare l'informazione tutelabile come segreto commerciale; in secondo luogo costituiscono il reale valore dell'informazione e l'effettivo stato di segretezza in cui essa si trova, determinando l'effettiva risposta agli altri due requisiti stabili sempre dall'art. 98 c.p.i. Tanto è vero che se l'informazione fosse liberamente disponibile sul mercato il valore intrinseco dell'informazione stessa sarebbe parimenti nullo o comunque molto inferiore, annullando il vantaggio competitivo ad esso collegato.

E' possibile distinguere due diverse tipologie di misure di protezione della segretezza delle informazioni: le misure denominate "endoaziendali", che si caratterizzano per un'applicazione e un esaurimento dei propri effetti all'interno della stessa impresa, e le misure definite come "esoaziendali", che sebbene generate all'interno dell'impresa, vengono adottate nel rapporto con soggetti terzi all'organizzazione imprenditoriale.

Queste misure atte a tutelare le imprese e i loro segreti hanno l'obiettivo di difendere l'organizzazione e le loro informazioni da tutti quei comportamenti illeciti volti

---

[141] Come indicato da A. OTTOLIA, (nt. 23), 1099, l'indagine sulla sussistenza di idonee misure di segretezza viene tradizionalmente svolta tenendo conto delle caratteristiche specifiche del soggetto che le possiede, sia su un livello quantitativo, che qualitativo, organizzativo e tecnologico, secondo criteri di adeguatezza relativa. Come indicato dalla giurisprudenza, è necessario identificare puntualmente il segreto per poter verificare l'adeguatezza dei requisiti. Si veda ad esempio Trib. Bologna, 23 novembre 2017, n. 2612, in *DeJure*. L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 510, supporta che la ragionevole adeguatezza delle misure è una nozione non assoluta, ma bensì relativa. Le misure devono essere quindi esigibili, la valutazione dovrà essere effettuata sul caso concreto, tenendo conto delle circostanze e valutando i costi delle misure in relazione alla loro possibile efficacia. Il concetto di esigibilità è da considerarsi perciò dinamico nel tempo, in quanto l'evoluzione tecnologica e l'andamento dei costi comportano una diversa valutazioni a seconda sia del periodo temporale dell'analisi posta in essere, che dell'adeguatezza o meno delle misure di protezione.

[142] In tal senso M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 56 e C. GARUFI, (nt. 42), 20.

all'acquisizione, rivelazione o utilizzazione di segreti commerciali. Questi comportamenti possono essere della più diversa natura, come atti indirizzati allo "spionaggio industriale" oppure violazioni da parte di un dipendente dell'impresa, sia in vigenza di un contratto valido o in un successivo momento. Una volta licenziato o dimessosi, infatti, la minaccia da parte di un ex dipendente potrebbe farsi più rilevante, in quanto, non essendo vincolato da nessun contratto, il medesimo potrebbe liberamente comunicare importanti informazioni dell'impresa ad un concorrente o ad un terzo soggetto esterno[143].

3.2. Strumenti endoaziendali

Abbiamo definito gli strumenti endoaziendali come ostacoli concreti o misure atte a proteggere le informazioni dell'impresa con una loro applicazione ed un proprio esaurimento all'interno dell'organizzazione dell'impresa. Questi strumenti sono predisposti in un'ottica di contrasto a quelli che sono comportamenti illeciti, limitando, o rendendo più difficile possibile, l'attuazione di condotte atte ad eseguire il c.d. "spionaggio industriale" o una qualsiasi acquisizione illecita di informazioni segrete[144].

Le misure endoaziendali volte a tutelare il segreto possono avere diverse forme, le prime che verranno presentate avranno una natura prettamente fisica: in questi casi l'impresa adegua una serie di veri e propri ostacoli fisici per rendere più difficile l'acquisizione del segreto. Queste tipologie di protezione possono essere molto diverse e adeguate a seconda delle risorse e delle

---

[143] Come evidenziato nello studio della Commissione Europea del 2011 sul segreto commerciale, presentato da V. FALCE, (nt. 2), 129, i dipendenti, gli ex dipendenti, i concorrenti e i fornitori sono tra i principali responsabili di violazione di segreti commerciali. Nei settori finanziari e delle telecomunicazioni le fonti di maggior rischio sono rappresentate da ex dipendenti, mentre in altri settori, come nel farmaceutico, nell'editoria e nei settori finanziari, le principali minacce provengono dai concorrenti dell'impresa. Lo spionaggio commerciale è una pratica che si afferma però prevalentemente nel settore meccanico e farmaceutico, settori in cui la percezione del rischio è aumentata nel corso degli ultimi 10 anni. Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 56 ss. e la Cass., sez. un., 27 novembre 2015, n. 24245, sentenza "Flaschenwerk Bebitz GmbH c. Acciaierie Valbruna s.p.a" in M. STELLA *corte di cassazione: decisioni di interesse procecessual-internazionalistico*, Ipsoa, 2016, 7, sentenza in cui una società italiana ha agito contro una diretta concorrente società tedesca, asserendo di essere stata vittima di atti di concorrenza sleale, consistenti nell'acquisizione illecita di progetti di know-how e di un elenco di clienti da parte di un proprio ex-dipendente dimissionario, in trattativa per passare alle dipendenze del gruppo straniero, a cui apparteneva l'impresa convenuta.

[144] Si veda Trib. Bologna, 13 novembre 2017, nella massima di P. PICARELLI, in cui si specifica che: "Non è infatti richiesta, a tal fine, l'assoluta inaccessibilità alle informazioni segrete, ma soltanto che la loro acquisizione non sia agevole, ad esempio, sul mercato ovvero tramite siti web dove sono reperibili informazioni di carattere generale e non personalizzate alle esigenze della singola azienda e che, quindi, sia necessario l'impiego di uno sforzo non ordinario". In tal senso si veda anche Trib. Torino, sez. spec. impresa, 15 novembre 2018, n. 5246, in *giurisprudenzadelleimprese.it* in cui si indica che: "Affinché un'informazione possa definirsi segreta non è necessario che sia inaccessibile, ma è sufficiente che la sua acquisizione sia soggetta a sforzi non indifferenti, superiori rispetto a quelli che occorrono per effettuare un'accurata ricerca". Queste misure di protezione devono essere già state adottate prima del processo da parte dell'impresa, dotarsi in vista dell'azione giudiziaria infatti poco servirebbe.

tecnologie a disposizione dell'impresa, se ne citeranno solamente alcune a titolo esplicativo[145].

L'organizzazione può adeguarsi, ad esempio, di sistemi di controllo degli ingressi nelle diverse aree dell'impresa, in particolare nelle zone produttive, in modo tale da sorvegliare i movimenti di soggetti esterni o del personale, permettendo l'accesso nei locali dell'impresa solo se provvisti di un eventuale e autorizzativo *badge* identificativo, rilasciato da organi preposti al controllo che vigileranno gli accessi. In aggiunta si potrà vietare la diffusione e l'effettuazione di filmati, foto, immagini, audio, scritti effettuati all'interno delle aree dell'impresa.

Un'altra forma di tutela endoaziendale può essere predisposta tramite la custodia delle informazioni segrete in depositi sicuri, monitorati e controllati, come in cassette di sicurezza, cassaforti, armadi blindati, o in tutti altri luoghi adibiti e predisposti a contenere la documentazione inerente informazioni riservate (quali disegni tecnici, dati di clienti, fornitori, prodotti ecc.), permettendo l'accesso a tali documenti al solo personale autorizzato, sotto disposizione degli organi di controllo.

Può risultare importante la definizione di procedure interne che dispongano una comunicazione delle informazioni segrete a seconda di un sistema di correlazione tra il livello o la posizione del dipendente all'interno dell'organigramma dell'impresa e il grado di confidenza e segretezza dell'informazione stessa; in tal modo la comunicazione di queste informazioni sarà limitata ad una cerchia quanto più ristretta possibile del personale interno all'impresa.

Le capacità di controllo della logistica e delle merci non comportano solo efficienza ed una riduzione dei costi, ma permettono anche un monitoraggio costante della posizione della merce e dei prodotti all'interno delle diverse aree dell'impresa, riducendo possibili acquisizioni illecite di informazioni contenute in esse. Proprio per questi scopi le imprese decidono sempre più di disporre di sistemi di controllo e certificazione del materiale, sia nelle zone di carico e scarico della merce, che nel magazzino e nei reparti produttivi. Si potrà così organizzare sistemi logistici con eventuali *barcode* e codici alfa-numerici allegati al materiale o alla merce, permettendo così un monitoraggio costante della loro posizione.

---

[145] Per un'approfondita analisi si veda S. BARBARO in G. RESTA, (nt. 48), 329 e G. CICCONE e F. GHINI, (nt. 75), 527. Il titolare di segreto commerciale deve adeguare l'impresa con una *policy* aziendale mediante il ricorso a misure che siano in grado di assicurare una efficace tutela fisica del segreto, con sistemi di protezione adeguati. Tutti gli esempi qui indicati sono presenti anche in M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 56.

Anche per ciò che concerne la documentazione si è reso sempre più necessario attuare un adeguamento del sistema tramite una classificazione dei documenti e delle informazioni dell'impresa. Le organizzazioni potranno così prevedere procedimenti di archiviazione e di marcatura della documentazione contenente dati sensibili con indicazione dello stato di segretezza, applicando ad esempio sul documento la stampigliatura "segreto", "riservato" oppure "*copyright*"[146].

Oltre alle misure fisiche fin qui illustrate il segreto commerciale può essere adeguatamente tutelato anche attraverso forme organizzative implementate nelle attività dell'impresa, rientrando sempre in quella categoria di misure che abbiamo definito come endoaziendali.

Nell'ambito dell'applicazione di alcune di queste forme organizzative, l'impresa potrà prevedere la definizione di *team* funzionali, come di ricerca e sviluppo, amministrazione, o marketing, disponendo l'accesso ai membri dei *team* a sole apposite aree o informazioni autorizzate. Importante può risultare anche l'individuazione di soggetti all'interno dell'impresa predisposti a concedere eventuali informazioni, know-how, merce, prodotti contenente dati sensibili o di natura riservata a soggetti interni o esterni l'impresa.

Infine la generazione di un ambiente di lavoro positivo, con sistemi chiari di regole e competenze, che mirino a riconoscere il lavoro svolto all'interno dell'organizzazione, attuando politiche retributive favorevoli al crescere di rapporti stabili anche tramite la sottoscrizione di patti di stabilità, possono limitare eventuali comportamenti negativi e illeciti di dipendenti che, comportandosi come vere e proprie "talpe", diffondono informazioni importanti a soggetti esterni all'impresa causando forti danni all'attività stessa[147].

Non risulta per nulla banale l'ultimo punto illustrato, sebbene l'ordinamento giuridico italiano preveda già all'articolo 2105 c.c. che: "*Il prestatore di lavoro non deve trattare affari, per*

---

[146] Si veda C. GALLI, *Le nuove frontiere del diritto dei brevetti,* Torino, Giappichelli 2003, 129. Come indicato da M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 58, per ciò che concerne la documentazione tecnica, è prassi nelle imprese utilizzare il "cartiglio" dei disegni tecnici o degli schemi tecnici di un impianto o macchinario in modo tale da registrare l'autore del disegno, la data di modifica o ulteriori indicazioni. Queste formalità possono venir ulteriormente integrate con idonee indicazioni riguardante la riservatezza delle informazioni del documento e della proprietà degli eventuali diritti connessi. In tal senso la giurisprudenza ha ritenuto valida la stampigliatura "segreto" su un documento come misura idonea a rendere quanto contenuto meritevole di tutela come segreto commerciale, indipendentemente dalla novità o dalle caratteristiche dell'informazione contenuta. Si veda in tal senso Trib. Milano, 31 marzo 2004, in *GADI*.

[147] In tal senso si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 136, dove si sottolinea l'importanza del "*job satisfaction*", in quanto rende possibile lo sviluppo di un sistema di prevenzione dell'infedeltà dei dipendenti. Si limitano così i rischi connessi alla sottrazione, da parte dei dipendenti, del know-how dell'impresa, informazioni che potrebbero venir comunicate a imprese concorrenti o sfruttate per scopi puramente personali. L'obiettivo ultimo è la generazione di un clima di fiducia, soprattutto nei confronti di quei lavoratori che hanno maggiori possibilità di attingere alle informazioni segrete dell'impresa.

conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio", così stabilendo un "obbligo di fedeltà" è in altre parole fondamentale che l'impresa attui tutti i possibili sistemi volti a garantire la fidelizzazione del dipendente, questo per limitare il rischio di potenziali comportamenti illeciti da parte del proprio personale.[148]

3.2.1. Strumenti endoaziendali verso ex dipendenti

L'obbligo di fedeltà del dipendente disciplinato dall'art. 2105 c.c. termina con l'interruzione del rapporto di lavoro, è quindi necessario per l'impresa valutare sistemi volti a garantire la fidelizzazione di ex dipendenti, in modo tale da garantire la riservatezza delle informazioni acquisite dallo stesso durante la sua permanenza all'interno dell'impresa.

Sorge qui la problematica nell'identificare gli strumenti che risultano più ideali per assicurare la tutela delle informazioni legittimamente acquisite dall'ex dipendente durante la sua permanenza presso l'ex datore di lavoro. Ed è questo un aspetto non irrilevante, giacché in questi casi posti in esame l'esigenza di tutelare il segreto si contrappone al principio secondo il quale l'ex dipendente e il suo nuovo datore di lavoro possono legittimamente utilizzare le conoscenze e le capacità tecniche e di mercato acquisite dal dipendente medesimo durante tutte le sue precedenti esperienze lavorative. La giurisprudenza ha più volte affermato che le esperienze acquisite nel corso del rapporto di lavoro del dipendente sono da considerare un suo esclusivo patrimonio professionale: una volta terminato il rapporto di lavoro, dunque, l'ex dipendente ha la piena facoltà di sfruttare tutte le conoscenze facenti parte del suo bagaglio culturale, questo principio ben si collega con il rispetto di quelli che sono i diritti inviolabili

---

[148] L'obbligo di fedeltà si applica a tutte le mansioni svolte dal dipendente all'interno dell'impresa in una qualsiasi forma contrattuale e tipologia d'inquadramento. L'obbligo di fedeltà del dipendente permane anche nei casi di temporanea sospensione dalla prestazione lavorativa, come nei casi di ferie, malattia e cassa integrazione. Si veda M. BARBIERO, *La tutela del know-how e il diritto del lavoro*, Politecnico di Milano, 2015. Nel *Commentario del Codice Civile Utet*, *Modulo Delle Persone, Vol. II* a cura di A. BARBA e S. PAGLIANTINI, 2019, 1363, si sottolinea che ai sensi dell'art. 90 G.D.P.R. gli obblighi di segretezza rilevanti possono derivare dal diritto dell'Unione, dal diritto degli Stati membri oppure da norme stabilite dagli organismi nazionali competenti. L'ultima ipotesi si ricollega alla normazione prodotta da organismi come gli ordini professionali. Analoga disciplina è contenuta nell'ambito del rapporto di lavoro in cui si richiamano i contratti collettivi, l'oggetto in questo caso è però rappresentato dal segreto professionale, ma anche da un obbligo di segretezza definibile "equivalente", in applicazione dell'ambito oggettivo della suddetta norma. Si veda anche G. CICCONE e F. GHINI, (nt. 75), 527, in cui si indica l'illecito utilizzo di segreti commerciali da parte di dipendenti e collaboratori durante la vigenza di un rapporto di lavoro subordinato e/o parasubordinato. Questi casi rientrano nell'alveo della violazione del dovere di fedeltà, come disposto dall'art. 2105 c.c. di competenza del giudice del lavoro, come indicato anche dal Trib. Torino, 13 marzo 2009, in *GADI*.

dell'individuo, quali la libertà di iniziativa economica e l'espressione della personalità[149]. Per dar luogo ad un illecito l'imprenditore dovrà dimostrare che le informazioni utilizzate dall'ex dipendente sono tutelabili come segreti commerciali, oppure che il comportamento della controparte è risultato contrario alla disciplina dell'art. 2598, co. 3, c.c. per quanto concerne la concorrenza sleale per sottrazione di segreti aziendali, ponendo così dei limiti all'utilizzo delle conoscenze del dipendente[150].

L'imprenditore, in ogni caso, può prevedere la costituzione di diversi strumenti endoaziendali, con l'obiettivo di evitare lo sviluppo degli eventi fin qui illustrati, ciò potrà essere attuato attraverso la sottoscrizione di contratti tra le parti, tra i quali i più diffusi e utilizzati si segnalano gli accordi di riservatezza e i patti di non concorrenza. Solitamente tali contratti vengono in essere durante il rapporto di lavoro, ma la loro applicazione è volta a tutelare le informazioni acquisite in particolare quando il rapporto tra le parti cessa di esistere[151].

L'accordo di riservatezza è un contratto atipico in cui l'oggetto dell'accordo tra il datore di lavoro e il dipendente è costituito da un obbligo di non divulgazione da parte di quest'ultimo di tutte quelle informazioni riservate acquisite durante la sua permanenza all'interno

---

[149] Si veda Cass., 13 novembre 1976, n. 4212, in *Dejure*, in cui si stabilisce che: "In assenza di un valido patto di non concorrenza, cessato il rapporto di lavoro e, con esso, l'obbligo di fedeltà di cui all'art. 2105 c.c., il lavoratore può, nello svolgimento della propria attività […] utilizzare le esperienze e le cognizioni tecniche acquisite a causa del lavoro svolto". Si veda anche M. BARBIERO, (nt. 148), 7. Le informazioni oggetto dei divieti stabiliti dall'art. 2105 non coincidono con le conoscenze apprese durante il rapporto di lavoro, che integrano la personalità professionale del lavoratore, consolidando quello che è il suo patrimonio intellettuale, così anche F. CARINCI, R. DE LUCA, TAMAJO, P. TOSI, T. TREU, *Diritto del lavoro 2. Il rapporto di lavoro subordinato*, Utet Giuridica, Torino, 2005, 245. Si veda anche Trib. Verona, 23 luglio 1998, in G. BONELLI, *Tutela del segreto di impresa e obblighi dell'ex dipendente,* in *Dir. ind.*, Ipsoa, 2002, I, 65, dove si indica che la tutela del segreto commerciale non può limitare la facoltà di sfruttamento, da parte dell'ex dipendente o di un ex collaboratore, di tutte le possibili conoscenze e competenze acquisite nella proprie pregresse esperienze lavorative.

[150] Come stabilito dalla Cass., 20 marzo 1991, n. 3011, in *GADI*: "Le capacità professionali che il dipendente abbia acquisito o migliorato nel corso del pregresso rapporto di lavoro costituiscono un suo esclusivo patrimonio professionale liberamente utilizzabile, mentre le conoscenze specifiche attinenti all'ambito riservato dell'altrui impresa permangono riservate e inutilizzabili in virtù delle regole di correttezza". Si veda A. VANZETTI, V. DI CATALDO, (nt. 48), 116 ss. Si veda anche P. MELI, *Note in tema di sfruttamento di informazioni da parte di ex dipendenti e collaboratori, in Dir. ind.*, 1999, 303, in cui si evidenzia l'impossibilità di ricorrere ad una regola generale, che sia posta di per sé a "dar ragione" al datore di lavoro o, piuttosto, all'ex dipendente, oppure viceversa. Risulta quindi necessario procedere con una valutazione di tutti gli aspetti interessati relativi alla vicenda, volta per volta.

[151] Si veda in tal senso il caso del Trib. Milano, sez. spec. in materia di imprese, 27 luglio 2016, in *DeJure*, dove s'indica che: "La società attrice alla fine del settembre 2013 avrebbe deciso di dotarsi di un'apposita sezione, denominata "Ricerca e Sviluppo", nella quale erano stati inseriti sei ingegneri, coordinati dall'ingegnere […] con la specifica mansione di procedere allo studio di nuovi macchinari medicali e all'aggiornamento di quelli esistenti; dal momento che tale attività inventiva non era mai stata regolamentata né esplicitamente retribuita, si sarebbe proposto agli ingegneri del reparto di sottoscrivere, a fronte di un aumento della retribuzione, un patto di riservatezza e di non concorrenza con cui si sarebbero impegnati per due anni dalla cessazione del rapporto di lavoro, a non svolgere alcuna attività lavorativa né in proprio né a favore di terzi nel settore della progettazione e sviluppo di apparecchiature medicali per la preparazione del sangue".

dell'organizzazione. E' necessario chiarite *ex ante* tutte le informazioni vincolate da questo accordo di riservatezza, non è possibile tutelare indirettamente tutte le informazioni senza specificarne alcune, in quanto l'accordo sarebbe nullo per illiceità e/o indeterminatezza del contratto. Oltre a ciò nell'accordo potranno essere definiti degli utilizzi leciti delle informazioni accordati al dipendente per scopi specifici, per utilizzi diversi da quelli approvati il dipendente dovrà sempre richiedere un autorizzazione al datore di lavoro. In ogni caso la validità o l'efficacia di questi accordi sarà maggiore quanto più verranno definite specificatamente le condizioni contrattuali e quanto più le informazioni da tutelare saranno determinate e ben descritte.

Questo strumento contrattuale può essere utile per preservare le informazioni dell'impresa nel tempo, l'accordo può infatti vincolare il dipendente a non diffondere le informazioni riservate per un periodo determinato o per un periodo indeterminato, mantenendo la propria efficacia anche oltre la fine del rapporto di lavoro, ogni violazione di tale accordo comporterà, per il dipendente, una possibile sanzione disciplinare, come stabilito dall'art. 2106 c.c., fino a determinare un possibile licenziamento, mentre all'ex dipendente potrà essere applicata una perseguibilità penale, scoraggiando quindi fortemente potenziali utilizzi illeciti delle informazioni oggetto dell'accordo[152].

Il secondo strumento endoaziendale che abbiamo citato è il patto di non concorrenza, disciplinato all'art. 2125 c.c., dove si stabilisce che: "*Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio*". Il patto, perciò, limita il dipendente nello svolgimento o nell'esercizio di un'attività lavorativa che possa essere in concorrenza con quella del datore, per una durata prefissata di massimo 5 anni (nel caso di dirigenti), o di altrimenti di 3 anni. Per la validità del contratto sarà richiesta la forma scritta, sarà inoltre necessario definire condizioni contrattuali specifiche, determinando un limite territoriale di valenza del contratto e un corrispettivo da erogare al dipendente in una forma variabile dal dieci al quindici

---

[152] Si veda M. BARBIERO, (nt. 148), 10. e M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 148 ss. Va precisato che il patto di riservatezza si traduce in una limitazione lavorativa o imprenditoriale del lavoratore, perciò conseguentemente e indipendentemente si dovrà in ogni caso applicare la disciplina in materia di patti di non concorrenza, anche se con i dovuti aggiustamenti. In assenza di un adeguato bilanciamento dei contrapposti interessi il patto potrà essere dichiarato in giudizio nullo e dunque privo di ogni effetto. Per questo risulta fondamentale la determinazione chiara dell'oggetto sottoposto a riservatezza e del preciso corrispettivo dovuto all'ex dipendente.

percento della retribuzione annua, ma in ogni caso proporzionale al divieto pattuito[153].

Il patto di non concorrenza risulta essere uno strumento più limitato rispetto alla tutela predisposta dall'accordo di riservatezza, sia per la protezione della segretezza delle informazioni acquisite dall'ex dipendente durante la sua permanenza nell'impresa, che per i limiti temporali, territoriali e i compensi economici stabiliti dalla disciplina. L'obiettivo principale del patto di non concorrenza è infatti la costituzione di un limite legale alla concorrenza più che la predisposizione di misure volte a rafforzare la tutela delle informazioni dell'impresa.

3.3. Strumenti esoaziendali

Abbiamo già evidenziato come le imprese, durante lo svolgimento delle proprie attività economiche, sviluppano una serie di rapporti con soggetti esterni all'organizzazione; per ottimizzare tali relazioni può essere necessaria un'intensa comunicazione tra le parti contenente informazioni relative l'attività produttiva. Particolarmente delicato è però il caso in cui la comunicazione tra le parti contenga, come oggetto, informazioni che l'impresa tutela e mantiene come segreti commerciali. Sorge dunque il bisogno per l'impresa di avvalersi di strumenti che siano in grado di garantire quanto più possibile il mantenimento dello stato di segretezza di queste informazioni, sebbene comunicate a soggetti esterni all'organizzazione.

Una soluzione a questa problematica può essere trovata tramite quegli strumenti che abbiamo già definito come esoaziendali, strumenti che l'impresa può utilizzare sia per esplicitare il carattere segreto di certe informazioni, sia per disciplinare tutti i rapporti con terzi soggetti esterni all'impresa, specificando determinate clausole che impongano l'obbligo, per questi soggetti, di mantenere riservate o segrete determinate informazioni a loro comunicate.

---

153 Si veda M. BARBIERO, (nt. 148), 11. In tal senso si è espresso il Trib. Bologna, 24 luglio 2007, n.7770, in A. ZAMA, S. CALVELLO, *Segreto - Tribunale di Bologna: concorrenza sleale per sottrazione di segreti e storno di dipendenti,* Filodiritto.it, 2017, reperibile in internet al seguente indirizzo: https://www.filodiritto.com/segreto-tribunale-di-bologna-concorrenza-sleale-sottrazione-di-segreti-e-storno-di-dipendenti#:~:text=Il%20Tribunale%20ha%20ritenuto%20sussistente,titolare%20delle%20stesse%20informazioni)%20e. In tal sentenza si rinviene la presenza di una denuncia da parte dell'attore di una sottrazione di informazioni riservate dopo aver precedentemente formalizzato con i propri dipendenti dei patti di non concorrenza**,** in cui si includevano clausole di riservatezza a tutela del know-how dell'impresa, in forza delle quali, si legge nella sentenza: "I lavoratori durante il rapporto di lavoro e successivamente per un periodo di tre anni erano tenuti a non divulgare e non utilizzare, per nessuna ragione o causa, notizie riservate della società attinenti all'organizzazione, ai metodi di produzione ed alle lavorazioni e tecnologie (know-how) incluso schemi hardware e programmi software, arrecando, indipendentemente dalle intenzioni, pregiudizio e danno, anche solo potenziale oltre che effettivo, all'azienda". A. ZAMA, S. CALVELLO commentando questa sentenza, specificano che il tribunale ha riconosciuto le tutele disposti dagli artt. 98 e 99 c.p.i., riscontrando la sussistenza di tutti i requisiti previsti dalla legge. Quanto alle misure di segretezza adottate, il giudice ha ritenuto pienamente idonee e adeguate le clausole di riservatezza contenute nei patti di non concorrenza determinate con i propri dipendenti.

Solitamente ciò avviene tramite delle pattuizioni di carattere contrattuale tra le parti, contenenti clausole che prevedano l'impegno, in forma scritta, della salvaguardia della segretezza delle informazioni, mediante l'istituzione di obblighi di non divulgazione a soggetti non autorizzati dei segreti comunicati durante lo sviluppo delle relazioni commerciali. Il soggetto che sottoscriverà tale accordo sarà così obbligato a conservare lo stato di segretezza dell'informazione; detto soggetto potrà essere ad esempio un fornitore, con cui l'impresa s'interfaccia per un contratto di fornitura, un cliente, a cui vengono comunicate certe informazioni sensibili, consulenti o collaboratori esterni, con cui l'impresa mantiene rapporti per usufruire dei loro servizi, o comunque altri soggetti che intrattengono relazioni con l'impresa e che li pongano in contatto con informazioni segrete. Tutto ciò limiterà il rischio di comunicare queste tipologie di informazioni a soggetti terzi, che comporterebbe il conseguente annullamento dell'effettivo valore del segreto, in quanto esporrebbe il segreto commerciale al pubblico dominio.

Come abbiamo già evidenziato, l'*open innovation* è un approccio sempre più diffuso nell'economia moderna, le imprese intrattengono relazioni con numerosi soggetti esterni provenienti da ogni parte del mondo, cosa che permette alle imprese di acquisire maggiori competenze, generare economie di scala e di conoscenza, accelerare il processo d'innovazione tecnologica. Allo stesso tempo però lo sviluppo di processi di *open innovation* ha visto aumentare anche il rischio per le imprese di essere vittime di attività volte alla sottrazione dei loro sforzi di innovazione e diffusione delle conoscenze riservate, con possibile acquisizione e sfruttamento economico di tali conoscenze da parte di soggetti non autorizzati[154].

Di conseguenza, le imprese hanno sempre più necessità di avvalersi di strumenti che permettano lo sviluppo di relazioni con soggetti terzi, limitando, allo stesso tempo, quanto più possibile i rischi connessi ad una possibile perdita delle informazioni segrete e i vantaggi competitivi a esse legati. Proprio per questo motivo le imprese utilizzano ampiamente strumenti esoaziendali, in particolare gli accordi di riservatezza (i c.d. *Non-Disclosure Agreement*) e accordi di non concorrenza tra imprenditori volti a limitare specifiche attività.

---

[154] Sarebbe l'abbattimento dei costi di collaborazione e di *networking,* la maggiore mobilità di scienziati e lavoratori della conoscenza a permettere la riduzione delle distanze tra gli attori dell'innovazione, parallelamente a ciò anche il trasferimento e l'integrazione dei processi di ricerca e sviluppo generano la creazione di asset condivisi, ponendo dunque la necessità, per l'imprenditore dell'innovazione, di minimizzare il rischio di perdita della propria conoscenza strategica utilizzata per lo sviluppo dei propri business, come sostenuto da M.A. SHILLING, F. IZZO, *Open innovation:l'impresa è un'opera aperta*, *Gestione dell'innovazione*, McGraw-Hill, 2017, 327 ss. Sul tema dell'*open innovation*, dei rischi e i vantaggi connessi a questo nuovo approccio, si veda anche H. CHESBROUGH, (nt. 21).

In particolare, nella prassi commerciale è diffuso l'impiego di accordi di non concorrenza, che prevedono la limitazione tra imprenditori di certe attività, il cui svolgimento può includere l'utilizzo di segreti commerciali. Tali accordi, come disciplinato dall'art. 2596 c.c., richiedono determinati requisiti, quali la forma scritta, la determinazione di specifiche temporali e territoriali, nel rispetto dei principi costituzionali di libera iniziativa economica[155].

Talvolta, gli imprenditori evitano di stipulare veri e propri accordi di riservatezza o di non concorrenza, soprattutto in casi di rapporti di fornitura tra PMI, poiché questi strumenti potrebbero risultare non del tutto adeguati a rapporti che si basano sulla fiducia personale, sulla familiarità della relazione, sia di carattere professionale che personale. È comunque necessario che in tutti i passaggi l'impresa sottolinei ed espliciti in modo chiaro alla controparte che determinate informazioni, benché resegli note, devono considerarsi riservate e utilizzabili in un circoscritto ambito specifico della relazione tra le parti. Resta poi il fatto che, al fine di garantire all'impresa l'effettiva possibilità di far valere i propri diritti in caso di violazione appare quantomeno opportuno, se non necessario, prevedere strumenti esoaziendali che prescrivano in modo chiaro e specifico la conservazione del carattere segreto delle informazioni contenute nelle comunicazioni tra le parti[156].

3.3.1. NDA (*Non-disclosure agreement*)

Per garantire la riservatezza delle informazioni fornite durante gli scambi commerciali la prassi conosce da tempo convenzioni e accordi che, come abbiamo già presentato, le controparti possono sottoscrivere per definire obblighi di riservatezza volti a mantenere inalterata la natura confidenziale dell'informazione.

---

155 Sull'argomento si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 81 ss., i patti di non concorrenza vengono però definiti come "l'ultimo baluardo", in quanto impongono dei vincoli di natura obbligatoria per via indiretta che incidono sia sul fine ultimo, come l'attività concorrenziale, che propriamente sul mezzo, ossia l'informazione segreta. È necessario che il patto che limita la concorrenza sia, in ogni caso, provato per iscritto, la sua validità dev'essere circoscritta ad una determinata zona oppure ad una determinata attività, non può in ogni caso eccedere la durata di cinque anni. Se la durata non viene determinata, oppure è stabilita per un periodo superiore ai cinque anni, il patto che limita la concorrenza è valido solamente per la durata di un quinquennio, come indicato da R. AMATORE in R. GIOVAGNOLI, *Codice Civile Commentato, Art. 2596 Codice Civile - Limiti contrattuali della concorrenza,* Giuffrè, 2015. L'intento perseguito dall'art. 2596 c.c. è di impedire eccessive restrizioni alla libertà di iniziativa economica mentre tutela il mercato nelle sue effettive strutture. Si veda in tal senso anche Corte Cost., 16 dicembre 1982, n. 223, in *Riv. dir. com.*

156 In tal senso si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 58 ss.; ciò non toglie che la prassi spesso non riconosce l'importanza dei passaggi sopra evidenziati. Infatti utilizzare lo strumento dell'accordo contrattuale risulta importante ogni volta che questo è destinato a specificare e regolamentare, seppur in parte o limitatamente in via collegata, tutti i diritti e gli obblighi relativi al know-how dell'impresa. L'accordo deve evidenziare, in particolare, la presenza di eventuali segreti commerciali, senza cadere in trappole tautologiche o clausole di stile che renderebbe oneroso e dispendioso il processo di sottoscrizione di tali accordi.

L'accordo di riservatezza è uno strumento che rientra sempre nelle misure che abbiamo definito come esoaziendali: tale accordo è infatti stipulato tra l'impresa detentrice di segreti commerciali e soggetti esterni con la quale la stessa impresa intrattiene determinati rapporti. Con la sottoscrizione di tale accordo si mira a regolare due interessi contrapposti: da una parte l'accordo soddisferà l'interesse della controparte di colmare l'asimmetria informativa che la separa dall'impresa, ricevendo, da questa, informazioni utili alla costituzione delle varie fasi del rapporto, dall'altro, l'impresa detentrice di segreti commerciali otterrà la garanzia che le informazioni fornite alla controparte saranno protette contro la divulgazione o l'indebito utilizzo di chi le riceve[157].

L'utilizzo di questi accordi può inserirsi all'interno di relazioni della più diversa natura, in particolare la loro sottoscrizione è diffusa nell'ambito di rapporti che prevedono la definizione di relazioni di tipo commerciale o rapporti di carattere economico tra operatori economici sofisticati, nelle quali intercorre lo scambio di informazioni aventi natura confidenziale. Tale accordo può comunque venir in essere anche in un qualsiasi altro momento o situazione che vede, in ogni caso, un soggetto terzo esterno all'impresa acquisire informazioni considerate segrete e che necessitano quindi della predisposizione di uno strumento, qual è l'accordo di riservatezza, volto a mantenere lo stato di segretezza di tale informazione[158].

Con la sottoscrizione dell'accordo vengono individuati due principali obblighi di non *facere*: *in primis,* le parti si obbligano a non utilizzare le informazioni per scopi estranei alle trattative o alla costituzione ed esecuzione del contratto; *in secundis,* le parti si obbligano a non divulgare le informazioni tutelate a soggetti non autorizzati[159].

---

157 Si veda P. ZANONI e L. CASATI, *La durata dei patti di riservatezza: dal termine di un obbligo di non facere al termine del diritto d'uso del bene informazione*, in *Contr*., 2018, V, 597.

158 Ad esempio M. FAZZINI, (nt. 77), evidenzia come durante l'effettuazione di attività di due diligence la diffusione, da parte della società target di informazioni sottoposte al controllo di due diligence può rappresentare un possibile *data breach*. Sicché l'autore segnala l'opportunità di adottare le opportune cautele quando vengono svolte queste tipologie di attività, ad esempio predisponendo una clausola ad hoc nell'ambito del *Non-disclosure agreement,* siglato a latere delle verifiche.

159 In tal senso P. ZANONI, L. CASATI, (nt. 157), 598 affermano che tipicamente gli accordi di riservatezza pongono in capo alle parti anche altri obblighi di non *facere* rispetto quelli già indicati. Si pensi, ad esempio, all'obbligo di non divulgare l'esistenza stessa di una trattativa commerciale in corso tra le parti oppure, piuttosto, l'obbligo della *receiving party* di non assumere o sollecitare in nessun modo i dipendenti della *disclosing party*. M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 66 ss., presentano ulteriori casi dove la costituzione di un accordo di riservatezza può risultare utile, come nelle già citate attività di *due diligence* oppure nelle indagini effettuate da parte di un'organizzazione presso un'altra, con lo scopo ultimo di acquisire tale attività economica o una parte di essa. Un altro esempio interessante presentato dagli autori è quello relativo alla valutazione congiunta di un progetto di ricerca e sviluppo, dove le parti conferiscono le proprie conoscenze e competenze. In tutti questi casi risulta indispensabile l'attuazione di uno strumento contrattuale che garantisca la tutela delle informazioni dell'impresa, com'è l'accordo di riservatezza.

L'accordo di riservatezza è una tipologia di contratto atipico, disciplinato in Italia dalla disciplina sui contratti in genere di cui agli artt. 1321 ss. c.c.; lo stesso ha però un'origine anglosassone e una diffusione in quegli ordinamenti, è infatti noto nel settore commerciale come NDA ossia "*Non-disclosure agreement*" o "*Confidentiality Agreement*" (in tal senso da ora si utilizzerà la terminologia NDA per riferirsi agli accordi di riservatezza)[160]. In inglese, l'accordo può venir tradotto letteralmente come "accordo di non divulgazione", questo sottolinea che il divieto di divulgazione non si estende alle sole informazioni tutelabili come segreti commerciali, bensì a tutte quelle informazioni che l'impresa ritiene riservate o sensibili, anche se prive dei requisiti richiesti per la tutela come segreto commerciale[161].

Abbiamo già detto come accordi di questo tipo vengano sottoscritti anche tra datore di lavoro e propri dipendenti, in questo caso però gli accordi rientrano nella tipologia di strumenti endoaziendali, che vengono utilizzati per predisporre tutele alle informazioni segrete acquisite dal personale interno all'impresa. Nei NDA la controparte all'imprenditore nella sottoscrizione dev'essere invece un soggetto esterno all'organizzazione dell'impresa.

Per evitare l'utilizzo di strumenti inadeguati le imprese tendono a sottoscrivere modelli di NDA standardizzati, ciò però potrebbe non bastare per garantire l'effettiva validità del contratto. E' infatti necessario che le parti identifichino i contenuti nel caso concreto, definendo specificamente come e quali informazioni saranno assoggettate al divieto di divulgazione, l'oggetto dovrà quindi essere chiaro e determinato perché l'accordo raggiunga lo scopo prefissato. Sarà inoltre necessario stabilire eventuali penali ed una durata di validità

---

160 P. ZANONI, L. CASATI, (nt. 157), 597 approfondiscono le locuzioni utilizzate nella prassi contrattuale per denominare gli accordi in esame, che risultano molteplici. Oltre alla locuzione accordo di riservatezza, si segnalano, senza alcuna pretesa di esaustività, altre locuzioni, come: "accordo di confidenzialità", "accordo di segretezza", "accordo di non divulgazione", "*confidentiality agreement*s" e "*secrecy agreements"*.

161 Come indicato da M. MASSINI, *Diritto al segreto e diritto alla riservatezza*, privacy.it, 2000, reperibile in internet al seguente indirizzo: https://www.privacy.it/archivio/massimi02.html#:~:text=La%20distinzione%20tra%20riservatezza%20e,la%20pubblicizzazione%20della%20notizia%20stessa. La differenza sostanziale tra informazioni segrete e informazioni riservate viene posta contrapponendo da una parte l'interesse al segreto, con ciò ci si impegna ad impedire che terzi soggetti vengano a conoscenza dell'informazione, e poi dall'interesse connesso alla riservatezza, vale a dire a precludere ogni tipologia di divulgazione o la pubblicizzazione dell'informazione stessa. La giurisprudenza ha espresso chiaramente cosa possa intendersi per informazione riservata, a riguardo si veda il Trib. Bologna, sez. spec. p.i., 04 luglio 2007, in *GADI,* in cui si afferma che: "Per informazioni riservate deve trattarsi di dati la cui raccolta almeno richieda sforzi superiori a quelli imposti da una accurata ricerca in letteratura, aventi oggetto notizie accumulate con lavoro individuale o di équipe, non surrogabile tramite la consultazione di materiali e di esperienze esterne, mentre il fatto che una pluralità di operatori sia in possesso di tali nozioni non toglie loro il carattere riservato, purché però il relativo numero risulti limitato e comunque venga mantenuto anche aliunde il necessario livello di protezione. Fra questi requisiti, infine, rilievo fondamentale assume il principio secondo cui informazioni del genere debbono inoltre essere mantenute secretate, adottando le misure di vigilanza che l'esperienza riconosce funzionali, e che valgano da ostacolo adeguato contro le violazioni che possano essere ragionevolmente previste e combattute".

dell'accordo, solitamente il termine è fatto coincidere con il momento in cui le informazioni oggetto dell'accordo cessano di avere un effettivo valore economico, ossia il momento in cui tali informazioni diventano generalmente accessibili oppure obsolete; si esclude invece la possibilità di prevedere clausole di riservatezza con durata indeterminata, in quanto determinerebbe un vincolo alla segretezza per un periodo di tempo eccessivo, comportandone l'effettiva nullità[162]. Frequentemente le parti stabiliscono anche clausole che limitano il divieto di rivelazione di determinate informazioni riservate a favore di certi soggetti autorizzati, ponendo quindi delle eccezioni, come verso taluni dipendenti di altre imprese o consulenti esterni[163].

Si prevede che una volta terminato il periodo di valenza dell'accordo di riservatezza il bene oggetto di tale accordo torni alla piena esclusiva disponibilità del suo unico proprietario iniziale, il quale potrà così riacquisire il diritto d'impedirne l'uso a terzi senza alcun limite di tempo, anche a chi, per un certo periodo, ne ha potuto fare uso, come stabilito per l'istituto del segreto commerciale[164].

3.4. *Assessment*, rischi e processi: fasi per la costituzione di un segreto commerciale

Abbiamo finora illustrato alcuni degli strumenti che le imprese possono sviluppare per costituire una protezione effettiva delle proprie informazioni segrete o delle proprie conoscenze verso quelli che possono essere degli utilizzi illeciti, illustrandone l'applicazione sia verso soggetti interni che esterni all'impresa.

---

[162] Ciò è ben evidenziato da P. ZANONI, L. CASATI, (nt. 157), 599, in cui, a tal proposito, indicano che nell'ordinamento italiano sussiste un generale divieto alla stipula di vincoli perpetui temporanei. La portata generale di questo divieto è sostenuto da un atteggiamento di assoluto sfavore da parte del legislatore non solo verso le tipologie di contratti stipulati in *perpetuum*, ma anche per tutti quei contratti stipulati pro tempore, ma con una durata temporale che risulta eccessivamente lunga. Secondo gli autori è quindi necessario che l'accordo di riservatezza (che è inteso essenzialmente come una fonte di un'obbligazione negativa) abbia una durata congrua all'oggetto e prestabilita dalle parti. Si veda anche M. MONTANARINI, *Contratti di cessione e di uso di know how e concorrenza sleale*, in *Contr. e impr*., 2007, IV-V, 1124, in cui si specifica che la penale dell'accordo dovrà essere commisurata dal possibile danno previsto. Al momento della redazione dell'accordo risulta inoltre utile un'accurata descrizione del know-how e delle informazioni ad oggetto, si impediscono così eventuali contestazioni da parte del cessionario, che possono essere sostenute prendendo per pretesto la nebulosità della descrizione dell'accordo. Un'accurata descrizione delle clausole contrattuali può però costituire un'arma a doppio taglio: se la descrizione dell'accordo dovesse giungere in possesso ad una controparte prima della stipulazione dell'accordo, il cedente rischierebbe di vedere l'oggetto di tale accordo divulgato. Si veda anche Cass., 22 aprile 2003, n. 6424, in G. CICCONE e F. GHINI, (nt. 75), 527.

[163] Si veda l'articolo di S. DE PALMA, *La protezione delle informazioni riservate: Non-disclosure Agreement e Confidentiality Clause,* filodiritto.it, reperibile in internet al seguente indirizzo: https://www.filodiritto.com/la-protezione-delle-informazioni-riservate-non-disclosure-agreement-e-confidentiality-clause#:~:text=L'oggetto%20del%20Non%2Ddisclosure,divulgarne%20a%20terzi%20il%20contenuto.

[164] Si vedano le conclusioni in P. ZANONI, L. CASATI, (nt. 157), 602.

La costituzione di efficienti protezioni richiede però l'attuazione di un processo di adeguamento delle misure, seguendo una serie di *steps,* che permetta una loro costituzione ottimale. L'impresa potrà così assicurarsi che le azioni intraprese per la tutela dei propri segreti rispondano ai requisiti richiesti dalla legge per la tutela dell'informazione come segreto commerciale. L'impresa, dunque, per applicare le misure fin qui illustrate, dovrà seguire un certo *iter*, che a parere di chi scrive, risulta fondamentale.

Innanzitutto sarà necessario che l'impresa svolga un attento e preciso inventario delle proprie informazioni, delle proprie conoscenze e dei dati a sua disposizione, dovrà poi selezionare i risultati di tale ricerca attentamente, selezionando solamente quelle informazioni che possono venir classificate realmente come dei possibili segreti commerciali; ciò verrà determinato in base ad una serie di caratteristiche, quali lo stato effettivo di segretezza dell'informazione e la capacità di rispondere ai requisiti stabili dall'ordinamento giuridico. L'impresa dovrà inoltre effettuare una valutazione di "costi-benefici": si prenderanno così in considerazione solamente le informazioni che danno un effettivo vantaggio competitivo, ossia quelle che, come stabilito dal secondo requisito del 98 c.p.i., hanno un effettivo valore economico in quanto informazioni segrete, ed oltre a ciò, sarà necessario stimare il costo dell'adeguamento delle forme di protezione, confrontando tale costo con i vantaggi connessi alla tutela dell'informazione come segreto commerciale: l'impresa dovrà dunque analizzare se tale investimento trova una sua giustificazione sotto il profilo economico e reddituale[165].

L'attività di inventario risulta fondamentale in queste prime fasi di formazione del segreto commerciale, in quanto permetterà di determinare la tipologia d'informazione e lo stato dell'arte, ossia l'avanzamento tecnologico in cui questa si trova: abbiamo già più volte sottolineato come i segreti commerciali possano avere diverse forme e natura (si pensi ad algoritmi nell'ambito di software più o meno complessi, informazioni frutto d'attività di

---

[165] Risulta però necessario precisare che sono diversi i motivi che possono spingere un'impresa a tutelare le proprie informazioni o conoscenze come segreto commerciale, e sostenere dunque i costi per il suo adeguamento. L'impresa dovrà quindi valutare tutti questi aspetti, oltre le motivazioni prettamente economiche e reddituali. Come presentato da V. FALCE, (nt. 22), 135, dallo studio sul segreto commerciale del 2011 proposto dalla Commissione Europea è emerso che in conseguenza all'acquisizione illecita di un segreto commerciale, le imprese temono in particolare una perdita di vendite (per il 56% degli intervistati), un aumento dei costi per le indagini interne (44%), maggiori spese per la protezione (35%), un aumento dei costi per la negoziazione degli accordi (34%), e dei costi per cause e processi (31%). Dallo studio risulta inoltre che le imprese temono, con la violazione di segreti commerciale, un danneggiamento alla reputazione e all'immagine della stessa impresa, una perdita dei vantaggi competitivi acquisiti negli anni, riduzione della tecnologia e della redditività. Tutte queste minacce potrebbero ridurre la volontà delle imprese nell'intraprendere attività transnazionali e di *open innovation* relative all'innovazione, *l'outsourcing* e gli investimenti.

ricerca e sviluppo, oppure ricette o metodi di produzione)[166]. Più l'impresa riuscirà a essere precisa nel definire il contenuto dell'informazione o della conoscenza che si vuole tutelare, maggiore sarà la capacità di proteggerla con misure di protezione efficienti.

Una volta terminata la fase d'inventario delle informazioni a disposizione e determinati gli eventuali benefici apportati dalla tutela, l'impresa dovrà analizzare attentamente il contesto in cui opera, valutando quali modifiche comporterebbe l'attuazione della protezione dell'informazione come segreto commerciale sia a livello interno, nella gestione della propria attività, che esternamente, nei rapporti con i soggetti terzi all'organizzazione.

Per ciò che riguarda le attività interne, sarà essenziale valutare se e come sono presenti, o si possono attuare, forme di protezione delle informazioni adeguate al caso, e che siano atte a mantenere le informazioni in uno stato di segretezza. Ciò verrà effettuato prendendo in considerazione sia le capacità a livello organizzativo e materiale già presenti all'interno dell'organizzazione, sia le capacità che possono invece venir sviluppate dall'impresa nel tempo o in fasi successive alla costituzione di un segreto commerciale[167].

Le forme di protezione richiederanno determinati investimenti, sarà dunque fondamentale per l'impresa definire fin da subito le proprie capacità, sia a livello economico che finanziario, per affrontare tali investimenti, che possono riguardare sia l'acquisto degli strumenti di protezione, sia il loro successivo adeguamento, mantenimento e manutenzione. É infatti importante evidenziare come le stesse attività di manutenzione possano avere una forte rilevanza, perché capaci di garantire che le misure di protezione non perdano completamente o parzialmente la loro efficacia, rischiando così di compromettere la segretezza delle

---

166 Come indicato da G. CICCONE e F. GHINI, (nt. 75), 526, nella pratica una delle maggiori difficoltà sta proprio nell'individuare chiaramente il know-how che si vuole proteggere: spesso l'imprenditore che si sente parte lesa fa riferimento ad un generico know-how, mentre risulta fondamentale, sia nella prassi, che prima e dopo un processo, la creazione di veri e propri "*corpora mechanica*", capaci di identificare eventuali segreti commerciali. Nel documento dell'European IPR Helpdesk, *Fact Sheet Trade secrets: An efficient tool for competitiveness,* 2017 si definisce chiaramente una lista di possibili informazioni tutelabili come segreti commerciali, questi sono ad esempio: metodi commerciali, analisi di mercato, rapporti d'affari, informazioni sui prezzi, sui costi sugli acquisti, dati personali, tecniche d'ufficio, elenchi di clienti e fornitori e relativi dati, informazioni finanziarie e pianificazione aziendale, dati di ricerca e sviluppo, know-how e tecnologia di processo, programmi e database per computer, formule e ricette. Come già visto, l'ordinamento giuridico italiano non pone limiti particolari al contenuto dell'informazione tutelabile come segreto commerciale, nonostante ciò l'impresa dovrà determinare con chiarezza l'oggetto dell'informazione, per assicura la costituzione di una tutela adeguata.

167 Abbiamo già illustrato diverse misure considerate come endoaziendali (si veda *supra* 3.2.), a tal proposito l'impresa potrà dunque valutare se dispone di modelli organizzativi capaci a limitare la fuoriuscita d'informazioni oppure sistemi di accesso ad aree o dati ai soli autorizzati. L'impresa potrà inoltre esaminare gli strumenti fisici o materiali a propria disposizione, come archivi o depositi di sicurezza, cassaforti, sistema di ingresso tramite *badge*, oppure tutte le misure capaci di tutelare l'informazioni all'interno di dispositivi informatici, come password o sistemi cifrati solo per citarne alcuni.

informazioni tutelate.

Una volta terminata la valutazione interna, l'impresa dovrà effettuare un'analisi accurata delle possibili implicazioni derivanti dall'utilizzo di segreti commerciali nelle relazioni con i soggetti esterni con cui l'impresa intrattiene certi rapporti. Per meglio definire ciò, deve essere considerato come l'applicazione di certe misure di tutela applicate alle informazioni o ai dati dell'impresa possa comportare delle modifiche nello sviluppo delle relazioni con terzi soggetti, delineando quali siano le misure di tutela più ottimali in quanto maggiormente idonee a non pregiudicare rapporti di fiducia consolidati[168].

L'impresa, nel valutare come l'apporto di strumenti di tutela comporti modifiche al contesto in cui opera, potrà utilizzare diversi approcci; ad esempio, si potranno valutare le conseguenze rispetto a quelle che sono definite come "forze di Porter", ossia esaminando come la costituzione di un segreto commerciale possa implicare dei cambiamenti nelle relazioni o nella forza contrattuale dell'impresa rispetto i propri fornitori, clienti, concorrenti, possibili produttori di beni sostitutivi o le nuove imprese entranti nel settore[169].

La costituzione di forme di tutela del know-how potrebbero infatti modificare fortemente il ruolo competitivo dell'impresa all'interno del proprio settore di riferimento: con una maggiore protezione delle proprie conoscenze specifiche, fonte di vantaggio competitivo, l'impresa riuscirebbe infatti a costituire maggiori barriere all'entrata, così facendo i nuovi entranti o i concorrenti già presenti sarebbero costretti a sostenere investimenti più significativi per realizzare un prodotto competitivo, in grado cioè di competere con quello dell'impresa detentrice di segreti commerciali. In tal modo, sia la minaccia di possibili nuovi concorrenti che l'intensità della concorrenza sarebbe minore e, in conseguenza a ciò, ci sarebbero maggiori possibilità per l'impresa di acquisire nuove quote di mercato.

Inoltre, una adeguata tutela del proprio know-how potrebbe generare per l'impresa una riduzione della dipendenza dai fornitori, aumentando così il suo potere contrattuale nei

---

168 In tal senso abbiamo già visto, presentando i NDA (si veda *supra* 3.3.1.), che non sempre questa forma di tutela è ideale, in particolare nei rapporti tra PMI: in questi casi infatti l'applicazione di NDA potrebbe minare un rapporto tra le parti basato sulla fiducia reciproca, è quindi necessario valutare altre forme di tutela. Bisogna precisare che in questo paragrafo ci si concentrerà nell'analizzare l'impatto del segreto commerciale sul rapporto con gli *stakeholder* esterni all'impresa, come clienti, fornitori, banche, azionisti, associazioni o istituzioni.

169 Si veda B. BERENSCHOT, in *Modelli di management. Idee e strumenti,* Prentice Hall, 2005, 44, dove si tratta del modello d'analisi competitiva di Porter sviluppato nel 1998. Questo modello identifica cinque forze fondamentali competitive, che determinano l'attrattività di uno specifico settore: nuovi entranti, forza negoziale dei clienti, forza negoziale dei fornitori, prodotti o servizi succedanei e la rivalità tra concorrenti esistenti. L'applicazione di questo modello può risultare utile per comprendere quali conseguenze ha un istituto giuridico, qual è il segreto commerciale, sullo stato competitivo dell'impresa e sul suo settore di riferimento.

confronti di questi soggetti. Se infatti le conoscenze di certe informazioni restassero di esclusivo dominio dell'impresa, la stessa potrebbe sfruttarle a suo più totale piacimento, senza sottostare a vincoli che potrebbero invece venir imposti dai fornitori se diversamente le conoscenze fondamentali non fossero pienamente in suo esclusivo possesso.

Il contesto e le conseguenze derivanti dall'applicazione di tutele derivanti dai segreti commerciali potrebbero essere analizzati attraverso strumenti di pianificazione strategici, come l'analisi SWOT. In tal modo l'impresa potrebbe determinare da un lato quali sono i suoi punti di forza e di debolezza, sempre inerente all'applicazione di forme di tutela delle proprie informazioni, valutando il grado di adeguatezza della struttura, potrebbe poi identificare eventuali opportunità e rischi legati all'attuazione di tutele specifiche delle proprie informazioni segrete. La valutazione dei rischi risulta fondamentale, in quanto permette di evidenziare possibili rischi connessi alla perdita dello stato di segretezza delle informazioni. Questi rischi possono consistere nell'acquisizione illecita delle informazioni segrete dell'impresa, ma anche nella distruzione, perdita, o modifica di tali informazioni[170].

Tutte queste attività che si sono descritte, dall'inventario, alla valutazione del contesto, alla determinazione dei rischi, dovrebbero venir svolte dall'impresa in quella che è una fase precedente e propedeutica alla creazione di un vero e proprio segreto commerciale, fase definita come "a*ssessment*"[171]. Questa fase può richiedere un'attenta e approfondita analisi da parte dell'impresa di tutti gli elementi indicati. La fase di *assessment* pone le basi per l'attuazione di una tutela efficiente del segreto commerciale, aiutando a definire adeguate misure di protezione, che siano in grado di rispondere ai requisiti richiesti dalla legge, adattando il segreto alla situazione in cui si trova ad operare l'impresa, rendendo il proprio know-how maggiormente protetto da tentativi d'acquisizione illecita da parte di soggetti non autorizzati.

---

[170] Per analisi SWOT (In inglese *Strengths, Weaknesses, Opportunities e Threats*) s'intende una valutazione dei punti di forza e di debolezza di un'organizzazione e le opportunità e rischi di un certo settore o di una situazione specifica. La valutazione del rischio può essere effettuata attraverso la procedura di *assessment* prevista per la valutazione d'impatto sulla protezione dei dati personali, o *Data Protection Impact Assessment,* denominata anche DPIA. Tale processo si articola sostanzialmente in tre operazioni principali: l'identificazione del rischio, l'analisi del rischio e la valutazione finale del rischio. Come indicato da B. PANATTONI, *Compliance, cybersecurity e sicurezza dei dati personali,* Ipsoa, 2020, 47.

[171] In inglese accertamento o valutazione. Nel Cambridge Dictionary si definisce come *assessment:* "The process of considering all the information about a situation or a person and making a judgment", ossia il processo di considerare tutte le informazioni su una situazione o una persona e di esprimere un giudizio. Questo processo viene utilizzato in diversi ambiti come in campo sociale e nelle risorse umane, nella valutazione della sicurezza, in ambito informatico ecc.

3.5. *Remediation*, misure adeguate

Una volta conclusa la prima fase di *assessment,* l'impresa dovrebbe aver portato a termine un'analisi completa delle proprie informazioni, del contesto applicativo e dei rischi connessi ad un'acquisizione, un'utilizzazione o una comunicazione illecita di una propria informazione potenzialmente tutelabile come segreto commerciale a soggetti non autorizzati.

Tutti gli aspetti evidenziati nella fase di *assessment* saranno fondamentali per la prosecuzione del processo di costituzione della tutela dell'informazione come segreto commerciale, il secondo *step* di tale processo è definito come fase di *"remediation"*[172]. In questa fase l'impresa dovrà valutare se le misure presenti sono idonee a proteggere il proprio know-how o come si possa migliorare ulteriormente la protezione, anche con eventuali strumenti o forme organizzative diverse da quelle già presenti, in modo tale da rafforzare la tutela secondo le indicazioni raccolte nella precedente fase di *assessment*.

L'impresa per effettuare questa valutazione potrà utilizzare diversi approcci e metodi, tra i più utilizzati si evidenzia la c.d. "*gap analysis*"[173]: con questo sistema l'impresa riuscirà a valutare sia gli strumenti di tutela già presenti, esaminandone le capacità di garantire la segretezza delle informazioni, effettuando inoltre un confronto tra gli detti strumenti di tutela e altri possibili sistemi che potrebbero venir successivamente implementati, destinati a migliorare o sviluppare maggiormente la tutela dei segreti presi in esame. La *gap analysis* potrà essere supportata da ulteriori calcoli dei costi di applicazione degli strumenti di tutela, dalla stima del livello di rischio di un'eventuale acquisizione illecita del segreto, si potranno poi analizzare i risultati in base agli obiettivi ottimali posti dall'impresa, misurando le prestazioni delle protezioni selezionate, verificandone l'efficienza e l'efficacia, ottenendo un'ulteriore confronto anche con quelli che potrebbero risultate i livelli potenziali d'utilizzo dei sistemi di tutela presenti e disponibili per l'impresa.

---

[172] Nel portale del Cambridge Dictionary viene definito come remediation: "The process of improving or correcting a situation", quindi un processo volto a trovare delle soluzioni pratiche a dei problemi concreti, questo termine viene spesso utilizzato nel settore chimico-industriale. Si veda anche S. FORTUNATO, C. DI NOCCO, *Corporate governance le fasi e i processi operativi di un'indagine interna o "internal investigation"*, in *Riv. dott. com,* 2018, LXIX, 233, in cui definisce *remediation* come: "L'implementazione delle azioni correttive necessarie, sulla base dei risultati dell'indagine interna".

[173] Tradotto dall'inglese *gap analysis* significa analisi degli scostamenti, ma più precisamente M. FAZZINI, (nt. 77), la definisce come il processo volto a determinare le possibili criticità di una certa situazione sottoposta all'attenzione, delineando e analizzando i necessari adeguamenti posti in essere che risulterebbero necessari.

L'impresa nella fase di *remediation* potrà anche effettuare degli "*stress test*"[174] sulle misure preposte alla protezione della segretezza delle informazioni: ciò è particolarmente importante per le informazioni conservate in formato digitale, come presso banche dati in *cloud*, software di sistemi gestionali o server. L'impresa potrà così testare il proprio livello di sicurezza e individuare eventuali falle nei sistemi per anticipare possibili attacchi e rischi futuri, così da prevenire eventuali accessi illeciti, accessi che potrebbero causare danni economici molto ingenti.

Le analisi qui presentate risultano di fondamentale importanza, perché grazie ad esse l'impresa riuscirà a identificare, dai risultati ottenuti, ulteriori misure per una protezione migliore ed efficiente dei propri segreti. Sarà però necessario che l'impresa pianifichi i processi qui descritti e la loro relativa implementazione in un *remediation plan,* che documenti e dia la possibilità di valutare, in un secondo momento, ogni passaggio effettuato per la costituzione della tutela dell'informazione come segreto commerciale.

Una volta conclusa la fase di *remediation* l'impresa sarà certa, o comunque potrà ragionevolmente ritenere di garantire il mantenimento dello stato di segretezza alle proprie informazioni, avendo predisposto delle misure di protezione adeguate a bloccare l'acquisizione illecita di tali informazioni a soggetti non autorizzati ed idonee a integrare il terzo requisito dell'art. 98 c.p.i. (ossia il fatto che le informazioni siano sottoposte "*a misure da ritenersi ragionevolmente adeguate a mantenerle segrete*").

In sintesi, la fase di *remediation* consente all'impresa di effettuare, fin dai primi momenti di costituzione della tutela, una valutazione dell'adeguatezza delle misure volte alla protezione del segreto commerciale: se infatti l'impresa non effettuasse un corretto approfondimento di questa fase il rischio sarebbe di incorrere in una costituzione di un segreto commerciale non tutelabile; elemento che si accetterebbe solo dopo un eventuale illecito e durante un processo, nel quale il giudice rilevasse l'impossibilità di applicare la tutela del segreto commerciale

[174] Con *stress test* s'intende la valutazione delle protezioni tramite dei procedimenti di prova effettivi del livello di sicurezza. Lo *stress test* è un'attività che viene effettuata in campi molto diversi, e con modalità a loro volta diverse; si evidenziano in particolare *stress test* nel sistema bancario, negli impianti nucleari e in informatica, dove si parla di *cyber security stress tes*t o di software *testing*.

perché in mancanza di uno dei tre requisiti richiesti dalla normativa[175].

3.6. Il monitoraggio

Terminata la fase di *remediation* l'impresa avrà effettuato un'analisi di tutte le misure di protezioni presenti e sviluppabili, con il fine di garantire il mantenimento dello stato di segretezza delle informazioni con misure adeguate al caso esaminato.

Abbiamo già illustrato nel paragrafo 2.5.1. come esistano notevoli differenze nei regimi di tutela tra i diversi istituti, come ad esempio tra segreto commerciale e brevetto. In particolar modo, mentre il brevetto si presenta come un elemento statico, difficilmente modificabile nel corso del tempo, per la complessità e i limiti posti da il procedimento di deposito, il segreto commerciale può invece evolversi e modificarsi più facilmente, la tutela dell'informazione potrà così ampliarsi di elementi e contenuti, facendo confluire all'interno dell'area di tutela ulteriori informazioni tutelabili come segreto commerciale in momenti successivi.

É sicuramente questo uno dei maggiori pregi del segreto commerciale: la mancanza di vincoli all'osservanza di determinate forme richieste dalla legge permette una facile integrazione ed un miglioramento del contenuto tutelabile con nuove e più aggiornate informazioni. Queste integrazioni possono essere frutto delle conoscenze acquisite nel tempo da parte dell'impresa o delle modifiche avvenute nel settore in cui la stessa impresa opera; sappiamo che

---

[175] Ed è questo un caso molto diffuso in giurisprudenza. In tal senso si veda la sentenza del Trib. Bologna, 27 luglio 2015, n. 2340, in *Giurisprudenzadelleimprese.it*, in cui il giudice stabilisce che: "Nel caso di specie, non è ravvisabile o, comunque, non è sufficientemente dimostrata, la sussistenza dell'ulteriore requisito richiesto dalla lett. c) dell'art. 98 c.p.i. In particolare, non vi è prova che la società attrice avesse predisposto dispositivi o presidii volti ad impedire l'accesso e la conoscenza dei dati tecnici riportati nei suddetti disegni, né che avesse quantomeno impartito specifiche direttive in tal senso. Infatti, pur trattandosi di patrimonio conoscitivo e tecnico di proprietà dell'attrice non agevolmente accessibile all'esterno e, quindi, riservato, non vi è prova che lo stesso fosse stato anche reso e mantenuto segreto nel senso in cui quest'ultimo termine è stato impiegato dal legislatore ed interpretato dalla giurisprudenza. Secondo la prospettazione difensiva dell'attrice, invece, il requisito in esame, di cui alla lettera c) dell'art. 98 c.p.i., dovrebbe ritenersi sussistente in ragione del fatto che le suddette informazioni tecniche e, segnatamente, i predetti disegni tecnici, erano custoditi in un personal computer privato, dotato di password ed in uso esclusivo al socio-amministratore e coprogettista. La circostanza allegata dall'attrice appare, tuttavia, insufficiente a conferire ai dati aziendali in esame il carattere della segretezza nell'accezione di cui alla lett. c) dell'art. 98 c.p.i.". L'impresa attrice non ha potuto quindi tutelare le proprie informazioni come segreti commerciali in quanto le misure adottate per mantenere inalterato lo stato di segretezza di tali informazioni sono risultate inadeguate. A parer di chi scrive, se fosse stata svolta un'attenta analisi di *remediation*, l'impresa si sarebbe accorta di tale mancanza e avrebbe corretto la situazione con delle misure adeguate al caso. Si veda inoltre la sentenza del Trib. Milano, 10 maggio 2016, n. 5791, in *Giurisprudenzadelleimprese.it,* dove il giudice ha diversamente rilevato che: "Nell'esame a campione dei dati sono stati reperiti sia codici sorgente proprietari, sia informazioni tecniche e commerciali classificate come confidenziali. Sotto questo ultimo aspetto, l'attrice ha peraltro fornito prova dell'adozione di misure idonee a mantenere segrete tali informazioni, con la predisposizione di un preciso protocollo di gestione della rete aziendale che prevedeva l'uso di password e di diversi livelli di accessibilità". Si può quindi sostenere che l'attrice, differentemente dal primo caso, ha potuto tutelare la propria informazione come segreto commerciale grazie all'adeguatezza delle misure poste alla tutela, e questo è probabilmente frutto anche di un'attenta analisi delle procedure in fase di *remediation*.

l'innovazione tecnologica è soggetta a numerosi e ricorrenti cambiamenti, le imprese perfezionano le proprie attività costantemente sviluppando nuove e più performanti conoscenze, il segreto commerciale è un istituto giuridico che, date le sue caratteristiche, ben si adatta a questa situazione. L'impresa potrà così introdurre miglioramenti al proprio know-how tutelato come segreto con procedimenti veloci e rapidi, senza la necessità di seguire procedure complesse che renderebbero l'integrazione un processo più complicato, come potrebbe avvenire per esempio nel caso di modifica del contenuto di un brevetto[176].

Questa capacità di evolversi da parte dell'istituto genera però anche la necessità per l'impresa di effettuare costanti e periodici controlli, per verificare il corretto mantenimento dello stato di segretezza dell'informazione anche dopo eventuali modifiche del suo contenuto. Proprio ricollegandoci a questo delicato aspetto, si può dunque sostenere che la procedura di costituzione di un segreto non termina con le fasi di *assessment* o *remediation,* ma bensì prosegue nel tempo, con mirate azioni di monitoraggio, capaci di garantire che le informazioni, benché modificate o aggiuntesi in un momento successivo al perfezionamento dell'istituto, rispondano sempre ai requisiti richiesti dalla legge per la tutela delle informazioni tecnico-aziendali come segreto commerciale[177].

Come già accennato, il monitoraggio dello stato di segretezza delle informazioni è un'attività indispensabile per ogni impresa che detenga segreti commerciali, e ciò vale anche per tutte imprese in cui non ricorrano nuovi elementi che integrano il proprio know-how tutelato. L'adeguatezza delle misure a protezione dello stato di segretezza dell'informazione può infatti cambiare e modificarsi nel tempo: ciò che si riteneva adeguato nel momento della costituzione del segreto e della sua tutela può non esserlo più con il passare degli anni, questo per le nuove tecnologie a disposizione o per l'obsolescenza delle protezioni costituite inizialmente.

E' proprio la costante innovazione tecnologia che può determinare una possibile obsolescenza degli strumenti di protezione, questo in particolare nell'ambito digitale, dove i miglioramenti registrati negli ultimi decenni sono stati significativi. Se l'impresa non effettuasse un

---

176 Si veda M. BONA, A. CAMUSSO, U. OLIVA, A. VERCELLI, (nt. 8), 40 ss. e S. SERAFINI, (nt. 20).

177 In tal senso si veda D. MASTRELIA, *La tutela del know-how, delle informazioni e dei segreti commerciali fra novità normative, teoria e prassi,* in *Dir. ind.*,, 2019, V, 523, in cui si sottolinea proprio che, analizzando alcuni casi giurisprudenziali, si riscontra una certa difficoltà da parte dell'imprenditore a provare le violazioni sulle informazioni tutelabili come segreti commerciali. Questo sarebbe dovuto soprattutto dal fatto che l'attore deve dimostrare la sussistenza di tutti i requisiti previsti dalla legge per la tutela del know-how e dei segreti commerciali. Risulta dunque fondamentale per l'imprenditore la predisposizione di un monitoraggio costante dello stato di segretezza delle sue informazioni per garantire lo stato di protezione nel corso del tempo.

monitoraggio costante dello stato di segretezza delle proprie informazioni non riuscirebbe ad accorgersi del possibile stato di obsolescenza dei propri strumenti di protezione, non rileverebbe neanche eventuali problemi di natura tecnica, i quali potrebbero richiedere un aggiornamento con delle versioni più attuali e performanti[178].

La realizzazione di un monitoraggio costante potrà consistere in attività indirizzate a verificare l'efficienza e la bontà delle misure di protezione adottate. Ciò dovrà essere eseguito regolarmente nel tempo, per evitare l'insorgenza di problematiche non prontamente risolte, sarà quindi necessario stabilire una calendarizzazione dei controlli, pianificando per tempo su quali misure e con che modalità effettuare detti controlli.

Risulta importante che il monitoraggio sia completamente documentato, in tal modo l'impresa riuscirà a mantenere la puntuale osservazione del livello di protezione dei propri segreti, attraverso appositi audit interni di tutti gli strumenti utilizzati, dettagliando una *check-list* che sia in grado di evidenziare rapidamente eventuali "falle" del sistema di protezione[179]. I risultati degli audit dovranno essere opportunamente trascritti, in modo tale sia da risolvere eventuali problematiche con azioni che risultino veloci e efficienti, sia per evitare l'insorgenza delle stesse problematiche in altre situazioni o in successivi momenti.

L'attività di monitoraggio potrà essere espressamente organizzata all'interno dell'impresa tramite delle procedure interne, dove possono essere indicati i principali responsabili della corretta esecuzione delle fasi di monitoraggio, con l'istituzione di comitati ad hoc, aventi compiti specifici di controllo e monitoraggio degli strumenti e delle metodologie di sicurezza, sia endoaziendali che esoaziendali; gli stessi comitati avranno anche la facoltà di proporre eventuali modifiche o miglioramenti delle misure a tutela dei segreti commerciali. Potranno inoltre essere previsti audit periodici di conformità per determinare il livello di protezione presente: le evidenze raccolte nel corso di questi audit dovranno dimostrare che i criteri di sicurezza sono adeguati a mantenere inalterato lo stato di segretezza delle informazioni e che i

---

[178] In tal senso si veda L. INNOCENTE in P. MARCHETTI, L.C. UBERTAZZI, (nt. 10), 510, in cui si sostiene che il concetto di esigibilità della protezione è da considerarsi in maniera dinamica e non statica. È quindi necessario un costante monitoraggio per definire il corretto rispetto dell'adeguatezza delle misure di protezione nel tempo.

[179] Il vocabolario Treccani definisce come *check-list* il linguaggio aziendale o la lista di voci che occorre controllare e spuntare per verificare che una determinata serie di attività o di processi risultino eseguiti in maniera corretta. A. QUARANTA, *Sistemi di Gestione Ambientale,* in *Amb. & svil.*, 2020, V, 446, descrive i *check-list* come documenti contenenti una serie di domande da porre e/o compiti da svolgere per evitare possibili dimenticanze. Questi documenti aiutano dunque a formalizzare eventuali non conformità riscontrate durante la conduzione degli audit.

requisiti richiesti dalla legge sono continuamente rispettati[180].

Oltre che per i motivi fin qui illustrati, l'attività di monitoraggio ha una funzione essenziale in quanto permette all'impresa di individuare celermente eventuali tentativi di acquisizione illecita di segreti commerciali. L'impresa potrà dunque, tramite costanti controlli dei propri sistemi di protezione, scoprire più velocemente se i propri sistemi di sicurezza sono stati violati da soggetti non autorizzati e, agendo rapidamente, limiterà gli eventuali danni derivanti dalla perdita dello stato di segretezza delle sue informazioni, tramite, ad esempio, azioni legali che richiedano la concessione di misure provvisorie e cautelari nei confronti del presunto autore dell'azione, così da limitare ogni tentativo di utilizzo e comunicazione delle informazioni segrete a terzi soggetti non autorizzati[181].

Dunque, concludendo la disamina delle fasi di formazione di un segreto commerciale, può sembrare che questo processo sia per certi versi complesso e dispendioso, sia a livello economico che per le tempistiche richieste, visto e considerato che, come indicato in questo paragrafo, l'attività di monitoraggio dovrà essere eseguita regolarmente nel tempo. Come spesso evidenziato in giurisprudenza, l'onere probatorio di violazione dei segreti commerciali può risultare difficile da assolvere, perciò la corretta esecuzione del processo volto alla costituzione di detto istituto giuridico risulta di fondamentale importanza per adottare tutti gli accorgimenti indicati dalla normativa vigente in una chiave che possiamo definire come "preventiva". Quindi il detto "prevenire è meglio che curare", nel caso della tutela dei segreti commerciali, è molto più di un semplice consiglio ma sintetizza il *modus operandi* che dovrebbe intraprendere l'impresa per costituire un'efficace tutela del know-how, delle informazioni e dei segreti commerciali[182].

---

[180] In tal senso si veda A. QUARANTA, *Professioni verdi: guida ai green jobs,* Wolters-Kluwer, 2021, 118.

[181] Nell'art. 10 della direttiva UE 2016/943 si stabilisce che l'autorità giudiziaria può, su richiesta del detentore del segreto, ordinare la cessazione o il divieto d'utilizzo o di divulgazione del segreto commerciale a titolo provvisorio, il detentore del segreto può inoltre vietare la produzione, l'offerta, la commercializzazione o l'utilizzo di merci costituenti violazione oppure vietare l'importazione, l'esportazione, o l'immagazzinamento di tali merci, anche prevedendo il sequestro o la consegna di tali merci. Le misure provvisorie e cautelari saranno più efficaci quanto più saranno prese tempestivamente, un costante monitoraggio dei sistemi di sicurezza e dei segreti potrà dunque aiutare l'impresa a scoprire celermente eventuali utilizzi illeciti dei suoi segreti o tentativi di acquisizione illecita, applicando le necessarie misure, che opereranno così in maniera più efficace. Si vedano anche gli artt.124 e 132 c.p.i.

[182] In tal senso si è espresso D. MASTRELIA, (nt. 177), 523, il quale aggiunge che per "curare giudizialmente" sarà comunque necessario dimostrare di aver adottato tutte le adeguate misure di prevenzione per la tutela delle informazioni, risulta quindi fondamentale aver eseguito correttamente tutti gli *steps* di costituzione del segreto commerciale presentati in questo capitolo.

PARTE II

CAPITOLO 4. IL SEGRETO COMMERCIALE E L'ECONOMIA DIGITALE

SOMMARIO: 4.1. Il settore digitale in Italia - 4.2. La valorizzazione del capitale intangibile - 4.3. Il legame tra segreto commerciale e settore digitale - 4.4. Strumenti digitali per la protezione dei segreti industriali - 4.4.1. *Blockchain* come sistema di tutela delle informazioni riservate - 4.5. Cenni su GDPR, normativa trattamento dei dati personali - 4.6. La normativa *cybersecurity* - 4.7. Cenni su *big data* - 4.8. Industria 4.0 e segreti commerciali - 4.9. Intelligenza artificiale e diritti di proprietà industriale - 4.10. Risvolti pratici per le imprese digitali.

4.1. Il settore digitale in Italia

E' opinione ampiamente diffusa che gli strumenti digitali giochino oggi un ruolo fondamentale e centrale nelle strategie di sviluppo economico delle economie moderne e delle organizzazioni produttive, hanno inoltre una funzione essenziale nello svolgimento e nello sviluppo delle attività quotidiane delle persone, incidendo così profondamente nella loro vita ma anche nella vita delle stesse imprese. Questo è principalmente dovuto alle molteplici capacità e opportunità offerte dalle tecnologie digitali, che ben si adeguano e rispondo alle necessità sia delle attività produttive, che della pubblica amministrazione, ma anche della collettività nel suo complesso. Bisogna sottolineare inoltre che le misure imposte per contrastare la pandemia di Covid-19 in Italia hanno accelerato il processo di trasformazione digitale già in atto; durante questo periodo, infatti, le tecnologie digitali hanno avuto un ruolo determinante e una diffusione sempre maggiore[183].

---

[183] La trasformazione digitale, o nella locuzione inglese più diffusa *"digital transformation"* viene spiegata da E. STOLTERMAN e A. CROON FORS, in *Information Technology and the Good Life, in Information Systems Research: Relevant Theory and Informed Practice*, 2004, 689 come un insieme di cambiamenti di natura prevalentemente tecnologica, culturale, organizzativa, sociale, creativa e manageriale associati con le possibili applicazioni di tecnologia digitale, in tutti gli aspetti della collettività. In tal senso si veda anche l'articolo di D. VITALI, *Covid-19 e sfida digitalizzazione, ultima chiamata per l'Italia*, IlSole24Ore, 2020, in cui si segnala che nel mese di marzo 2020, *l'e-commerce* è cresciuto del 20% rispetto a marzo del 2019, del 28,2% ad aprile, registrando a maggio 2020 un balzo del 41,7% (secondo dati Istat). Nel 2020 le vendite online hanno avuto un aumento complessivo tra il 35% e il 40%, sempre rispetto al 2019. Come sostenuto da D. VITALI, questi dati dimostrerebbero come l'approccio delle persone nei confronti del settore digitale è molto cambiato nell'ultimo anno. Il *lockdown* prima e il distanziamento sociale poi hanno infatti innescato un'evoluzione nelle abitudini dei consumatori, che in Italia ha anticipato il mercato, trainando poi anche imprese e istituzioni. L'autore aggiunge che è necessario ritenere la digitalizzazione oramai strategica in ogni settore dell'economia e, in particolare, le tecnologie digitali e i dati devono diventare la base su cui costruire una nuova pubblica amministrazione.

Tuttavia tale processo in Italia registra un ritardo rispetto al livello di sviluppo presente negli altri paesi europei, l'Italia risulta infatti quartultima fra i 28 paesi nella classifica Desi (Digital Economic & Social Index), l'indice con cui la Commissione Europea monitora lo stato di digitalizzazione dei paesi membri. Nell'ultimo periodo però il processo di *digital transformation* ha visto, in particolare nel nostro paese, una forte crescita: dal Digital Transformation Index 2020 di Dell Technologies è emerso che oltre l'85% delle imprese italiane ha accelerato il processo di digitalizzazione dei processi produttivi nel 2020, un dato superiore alla media europea, che si attesta invece al 75,3%; il dato italiano risulta superiore anche a quello registrato in nazioni fortemente sviluppate a livello tecnologico, come Germania (71,7%) e Francia (70,7%)[184].

Il processo di trasformazione digitale consente lo svolgimento di un sempre maggior numero di attività sfruttando il potenziale delle tecnologie digitali: si pensi allo *smart-working,* alla scuola a distanza, agli acquisti online, agli eventi in *streaming,* alla dematerializzazione e alla remotizzazione dei processi produttivi. Tutt'ora però, secondo le considerazioni di Marco Gay, Presidente di Anitec-Assinform, "*la digitalizzazione appare inattuata nelle sue vere potenzialità, infatti non deve basasi nel solo tradurre semplicemente in digitale ciò che è fisico, ma di trasformare i processi, il modo di pensare il lavoro e la produzione, i servizi sanitari, la produzione e l'erogazione dei servizi pubblici, il modo di insegnare ai nostri giovani e non solo il mezzo che sia una lavagna o un PC"*[185]. La trasformazione digitale è quindi un processo ancora in piena fase di sviluppo e attuazione nel nostro paese e, nonostante i notevoli passi in avanti fatti negli ultimi anni, le nuove applicazioni e il progresso della tecnologia digitale possono generare ulteriori utilizzi, comportando così delle successive

---

[184] Si vedano i risultati della ricerca di Dell Technologies dal sito: https://www.delltechnologies.com/it-it/perspectives/digital-transformation-index.htm. La Commissione Europea, nel Digital Economy and Society Index (DESI), in italiano Indice di digitalizzazione dell'economia e della società, misura il livello di digitalizzazione dell'economia e della società. Come riportato dall'indice, l'Italia è passata da un livello di 28,9 nel 2014 a 43,9 nel 2019, ancora però sotto la media europea, che si colloca a 52,5. L'Italia si posiziona così solo al 24° posto nella graduatoria, davanti a Polonia, Grecia, Romania e Bulgaria. L'indice valuta cinque aspetti a livello macro per costituire il livello di digitalizzazione del paese, solamente in due ("connettività" e "servizi pubblici digitali") l'Italia ha migliorato negli ultimi anni e presenta un livello vicino alla media europea, mentre nei restanti tre ("capitale umano", "uso di internet" e "integrazione della tecnologia digitale") l'Italia registra un forte ritardo. Commentando tale situazione, Cesare Avenia, presidente di Confindustria Digitale, in occasione dell'audizione presso la Commissione Lavori Pubblici del Senato, ha affermato che tale posizione sarebbe in assoluta contraddizione con l'essere l'Italia fra le economie più industrializzate al mondo, riflettendo ampiamente il ritardo tecnologico, economico, organizzativo e culturale del nostro paese.

[185] Anitec-Assinform è l'Associazione nazionale delle imprese ICT e dell'elettronica di consumo legata a Confindustria, racchiude al suo interno 700 associati appartenenti al settore dell'*information and communication technology* che operano sul mercato italiano.

profonde modifiche e possibili miglioramenti alla vita quotidiana delle persone e all'attività economica delle imprese e della pubblica amministrazione.

Quando si parla di mercato digitale, secondo la ricostruzione di Anitec-Assinform, ci si riferisce a quattro macro aree di prodotti e servizi in ambito digitale: nella prima categoria rientrano i dispositivi e i sistemi digitali, come dispositivi per la casa e l'ufficio (Pc, videogiochi), gli *enterprise e specialized system* (sistemi di *storage,* server) e i *personal e mobile device* (*smartphone, tablet, laptop* pc). La seconda categoria comprende i software, che si possono suddividere in software di sistema, software *middleware* e software applicativi e le soluzioni ICT, ossia le tecnologie dell'informazione e della comunicazione[186]. La terza categoria racchiude i servizi ICT, tra i quali si registrano servizi di *data center,* servizi di *cloud computing, Outsourcing ICT,* servizi di consulenza e servizi di rete che si possono a loro volta suddividere in servizi di rete fissa e mobile. Infine, la quarta categoria comprende il comparto dei contenuti e della pubblicità digitale, come *news online, gaming, mobile entertainment* e *digital advertising.*

Dai dati riportati nel rapporto di Anitec-Assinform, "Il Digitale in Italia 2020, Volume II", si evidenzia come il mercato digitale italiano ha mostrato una forte resilienza in un contesto di forte pressione dovuto alle chiusure forzate di imprese e imposizioni dettate dall'emergenza sanitaria. Nei primi sei mesi del 2020 il settore digitale ha fatturato 33.916 milioni di euro, con un leggero decremento del 2,9% rispetto allo stesso periodo dell'anno precedente.

Analizzando singolarmente le 4 macro aree di cui si compone il mercato digitale, si può notare che solo il settore dei contenuti e della pubblicità digitale non ha subito una flessione nei ricavi, attestandosi sui 6.013 di euro di fatturato e una crescita totale del 2,6%, mentre le altre 3 macro aree segnano dei lievi risultati negativi. Il comparto dei dispositivi e dei sistemi ha avuto, nel 2020, una contrazione del 2,6%, con un fatturato totale di 8.624 milioni di euro; il settore dei software e delle soluzioni ICT segna un decremento del 4,6% per un totale di 3.402 milioni di euro; infine, i servici ICT, nel primo semestre 2020 registrano 5.786 milioni di euro di fatturato, con un calo complessivo del 2,3% mentre i servizi di rete, con un mercato di 10.092 milioni di euro, hanno subito la contrazione maggiore, del 6,1%, registrando

[186] I software di sistema sono relativi al sistema operativo dell'elaboratore elettronico, da definizione Treccani. I software *middleware,* come indicato dell'Enciclopedia Britannica, sono software che consentono la comunicazione tra più applicazioni software, possibilmente in esecuzione su più di una macchina. Infine i software applicati sono programmi applicativi progettati per particolari funzioni, come possono essere ad esempio la scrittura, l'elaborazione di immagini, la gestione dei dati ed altro ancora, come indicato nel vocabolario Treccani.

andamenti in calo sia nei servizi di rete fissa che nella rete mobile.

Durante il primo semestre, tranne per Internet of things o IoT[187], tutti i *digital enablers* hanno mantenuto un trend positivo, queste tecnologie hanno infatti svolto un ruolo importante nel gestire le criticità dell'emergenza sanitaria, come il *cloud computing, l'artificial intelligence* e la *cybersecurity.* In particolar modo la *cybersecurity* segna una forte crescita del 7%: vedremo proprio nei prossimi paragrafi come questa tecnologia sia fondamentale per la tutela dei segreti commerciali, tanto è vero che le imprese hanno mantenuto o addirittura ricorso ad un extra budget per gli investimenti in *cybersecurity* negli ultimi anni, prevedendo maggiori spese ad esempio per sistemi di protezione del lavoro da remoto e degli ambienti in *cloud*, questo anche dovuto all'aumento dei *cyber*-attacchi.

Secondo le previsioni riportate sempre nel rapporto di Anitec-Assinform, nel 2021 si prevede una ripresa complessiva del mercato digitale italiano, con una crescita del 3,4%, con 72.955 milioni di euro di fatturato totale per l'intero comparto, un miliardo in più rispetto al 2019. Per il 2022 si prevede una conferma della crescita del 3,3%, superando complessivamente i 75.000 milioni di euro di fatturato. Per il biennio è prevista una crescita di tutte e quattro le macro aree ad eccezione dei servizi di rete, che continueranno a seguire il trend degli anni precedenti. In particolar modo Anitec-Assinform evidenzia che una crescita caratterizzerà lo sviluppo dei *digital enablers,* grazie all'evoluzione della *data strategy* e delle soluzioni *big data,* in particolare nelle grandi organizzazioni, che sfrutteranno così sempre più i propri dati aziendali. La crescita della digitalizzazione e delle attività in rete renderanno necessario l'adozione da parte delle organizzazioni di strumenti di protezione e, in tal senso, la *cybersecurity* segnerà un forte sviluppo, poiché le minacce di possibili attacchi informatici saranno sempre maggiori e i sistemi utilizzati sempre più sofisticati, rendendo più rischiosa la conservazione e l'analisi di dati e di sistemi operativi, così da costringere le imprese a incrementare gli investimenti in *cybersecurity* per garantirne la sicurezza[188].

Il settore digitale gioca un ruolo chiave nel Bilancio Pluriennale 2021-2027 dell'Unione

---

[187] Si veda in tal senso *Significato di internet of thinking*, Inside marketing, 2020, reperibile al seguente indirizzo: https://www.insidemarketing.it/glossario/definizione/internet-of-things/. L'internet delle cose, acronimo in inglese dell'Internet of things (IoT), è l'espressione utilizzata per descrivere l'estensione della connessione a internet delle più svariate tipologie di oggetti (dagli elettrodomestici alle auto).

[188] A. DI CORINTO nell'articolo *Il cybercrime è la terza economia mondiale. "10 milioni di danni dal secondo",* LaRepubblica, 2021, precisa che i danni provocati dai soli attacchi *ransomware*, secondo CybergON, arriveranno a 20 miliardi di dollari nel corso del 2021. Questo fenomeno sarebbe collegato all'aumento esponenziale della "superficie di attacco": entro il 2023 infatti il numero di dispositivi connessi alla rete internet triplicherà, mentre la sicurezza della tecnologia 5G, che metterà in rete case e uffici, non è stata ancora ben definita.

Europea, l'UE ha programmato forti incentivi per dare impulso all'economia comunitaria in risposta alla crisi causata dalla pandemia. Con il pacchetto Next Generation EU, in particolare, sono stati previsti fondi agli Stati membri fino a 780 miliardi di euro, quote importanti di questo pacchetto sono state destinate proprio allo sviluppo di strumenti digitali. Inoltre, con il piano Digital Europe, la Commissione Europea ha stanziato 9,2 miliardi di euro a sostegno dello sviluppo in Europa delle conoscenze e delle capacità digitali delle più diverse aree avanzate dell'ICT, come *artificial intelligence, cybersecurity* e *digital transformation*[189].

Il settore digitale dunque, nonostante le difficoltà economiche del periodo, sta continuando a crescere, diventando uno dei settori centrali nello sviluppo delle attività economiche e dei sistemi produttivi mondiali. Grazie alle sue numerose applicazioni, alla possibilità di ulteriori sviluppi tecnologici e ai fondi europei stanziati il settore digitale potrà rafforzare ulteriormente il trend positivo registrato negli ultimi anni, garantendo ai *players* del settore la possibilità di vedere le dimensioni dei propri business aumentare progressivamente.

4.2. La valorizzazione del capitale intangibile

I beni intangibili sono il frutto delle attività di ricerca e sviluppo, dell'esperienza e dell'ingegno umano e, nel sistema economico moderno risultano fondamentali in quanto permettono l'acquisizione di competenze e conoscenze uniche, fonte di vantaggi competitivi. Sono ritenuti per questo asset sempre più rilevanti e centrali per lo sviluppo, essendo un vero motore dell'economia moderna per le attività produttive, la pubblica amministrazione e per la collettività in generale.

Permane tuttavia ancora ad oggi il problema di trovare una giusta collocazione economica a questi capitali che, rivestendo nelle scale delle priorità imprenditoriali posti primari, hanno necessità di trovare delle giuste indicazioni negli indici collegati al patrimonio intangibile, permettendone così la salvaguardia e, allo stesso tempo, una valutazione economica che sia in grado di valorizzarne correttamente la generazione di valore di questi asset.

---

[189] Il Bilancio UE tra i suoi capitoli con dotazioni dedicate al digitale annovera Horizon Europe (HE), Connecting Europe Facility (CEF), InvestEU. Nella politica di coesione, che vale circa un terzo del bilancio della UE, 2 dei 5 obiettivi prioritari (Smarter Europe e More Connected Europe) riguardano connettività digitale, innovazione e digitalizzazione. E' previsto un programma finanziario ad hoc, Digital Europe 2021-2027, con una dotazione finanziaria di 6,76 miliardi di euro a prezzi correnti. Il programma Digital Europe si fonda su cinque pilastri**:** *High Performance Computing* (HPC), Intelligenza Artificiale, *Cybersecurity*, Competenze Digitali Avanzate (in particolare per *Cybersecurity*, HPC, IA), Impiego ottimale della Capacità Digitale e Interoperabilità. Tutti i dati presentati in questo paragrafo sono estrapolati dal rapporto Anitec-Assinform, *Il Digitale in Italia 2020, Volume II,* 2020, 23.

I beni intangibili hanno come caratteristica principale e identificatrice il loro stato d'immaterialità, differenziandosi, perciò, da quel patrimonio definito come tangibile o materiale dall'impresa. Sebbene il valore dei beni intangibili non sia secondario al valore del patrimonio materiale è ancora oggi diffusa l'idea di applicare una vera e propria valutazione economica ai soli beni che possono venir toccati e mostrati e, dunque, ai soli beni materiali, mentre i beni intangibili, dato il loro stato immateriale, vengono rappresentati nel capitale dell'impresa come quel "patrimonio invisibile" che costituisce l'insieme di conoscenze per definire soluzioni pratiche al cosa e come fare[190].

È necessario precisare inoltre che, data l'eterogeneità e il vasto ambito dei beni intangibili, non è facile identificare tutti i capitali dell'impresa che possono risultare tutelabili come asset intangibili. Sintetizzando, si possono però suddividere i beni immateriali in tre diverse tipologie: le prime due categorie godono di protezioni di natura legale e, nel loro ambito, si possono ritrovare i diritti di proprietà industriale come brevetti, marchi registrati, segreti industriali e i beni di proprietà intellettuale come il diritto d'autore. La terza categoria raggruppa invece tutti gli asset intangibili che potremmo definire "competitivi", ad esempio il capitale umano, i sistemi d'efficenza dei processi organizzativi e produttivi, le capacità di generare innovazioni, tutti elementi che possono determinare il livello di performance di un'impresa: in altre parole il know-how. L'esclusione dell'ultima categoria da possibili tutele giuridiche risulta comunque una visione superata, come dimostrato dai nuovi modelli economici introdotti dalla UE sulla redazione del bilancio aziendale, dove vengono incorporati i beni intangibili tra le voci rappresentanti il patrimonio fisico o finanziario dell'impresa. Questo prova il fatto che gli asset intangibili sono oramai una fonte di ricchezza e godono di un'importanza sempre maggiore, permettendo alle imprese di perseguire i propri obiettivi. Dalle ultime rilevazione si calcola che i posti di lavoro generati in Italia da imprese che sfruttano il potenziale del capitale intangibile sono circa 7 milioni, rappresentando il 31,5% dell'occupazione nazionale. La stessa UE si è posta come obiettivo la generazione di un'economia più competitiva tramite una regolamentazione più attenta dei diritti di proprietà

[190] In tal senso si esprime anche E. SALVATORE, (nt. 76), 29. Il vocabolario Treccani definisce come bene immateriale tutto ciò che non è materiale, non formato quindi di materia. Nel linguaggio economico, questo comprenderebbe: l'ingegno, la capacità professionale o l'abilità tecnica di una persona in quanto fonte di ricchezza. In diritto invece include: cose o beni che non hanno un'entità materiale o sensibile, pur avendo un contenuto patrimoniale (come per esempio, i prodotti dell'ingegno umano nelle svariate forme della produzione scientifica, artistica o letteraria). Simile definizione è presentata per gli asset intangibili, secondo l'illustre vocabolario Treccani questi costituirebbero il capitale intellettuale, che non può essere né visto, né toccato o misurato, non incorporato nel patrimonio fisico o finanziario dell'impresa.

intellettuale, in quanto strumenti in grado di generare ricchezza e una maggiore occupazione, stimolando in questo modo un mercato più competitivo a livello mondiale[191].

La consapevolezza, nel mondo economico, che le risorse intangibili sono fonte di vantaggio competitivo e permettono una maggiore efficienza è oramai diffusa, ne sono conferma di ciò gli investimenti delle imprese nello sviluppo di asset immateriali, sempre più frequenti e importanti. Le imprese possono inoltre generare un ritorno economico dagli investimenti effettuati, sia sotto forma di riduzione di costi, sia come maggior valore delle loro attività[192].

Le innovazioni originate dallo sviluppo degli asset immateriali sono sempre più numerose e permettono di adeguare meglio l'attività delle imprese a quelle che sono le esigenze dei mercati internazionali. Tanto è vero che in molti campi economici la rilevanza dei beni immateriali ha raggiunto o addirittura superato l'importanza dei beni materiali e ciò è vero non solo per quelle realtà imprenditoriali ad alto contenuto tecnologico, bensì anche per quelle attività definibili come "tradizionali"[193].

La crescente importanza del capitale intangibile rende necessario analizzare come questo patrimonio debba essere trascritto correttamente nelle poste di bilancio, valutandone il valore con stime che siano più realistiche possibili; in tal senso abbiamo già visto i riflessi sulla

---

[191] I dati sono riportati nel libro di E. SALVATORE, (nt. 76), 30. Nella relazione elaborata in collaborazione tra EPO e l'Ufficio dell'UE per l'analisi delle industrie ad alta intensità di diritti di proprietà intellettuale, in relazione ai risultati economici nell'UE, si indica come l'innovazione sia una delle principali tematiche di "Europa 2020": la strategia di crescita decennale adottata dall'UE è intesa così a creare un'economia più competitiva, con livelli occupazionali più elevati. Il raggiungimento di questo obiettivo dipenderà da diversi aspetti, tuttavia, un efficiente sistema in materia di diritti di proprietà intellettuale rientrerà certamente tra i più importanti fattori di crescita, data la capacità della proprietà intellettuale di incoraggiare la creatività e l'innovazione a livello dell'intera economia dell'Unione. L'Europa può però vantare in questo settore una lunga tradizione: gli Stati membri dell'UE e dell'Organizzazione europea dei brevetti hanno rivestito un ruolo primario nel plasmare un sistema di diritti di proprietà intellettuale che risulta allo stesso tempo moderno ed equilibrato, non solo garantendo agli innovatori il giusto compenso, ma stimolando parimenti anche un mercato competitivo. Nell'economia attuale, caratterizzata da mercati sempre più globalizzati e dal ruolo centrale della conoscenza, è di vitale importanza garantire che questi sistemi rimangano efficaci per l'attuazione di nuove e più strutturate politiche di innovazione. Si veda anche M.S. AVI, (nt. 77), 94 per la ripartizione delle categorie dei beni intangibili.

[192] Si veda V. CARLINI, *Wall Street, il dominio degli asset intangibili tocca i 35mila miliardi,* IlSole24Ore, 2020. in cui si sottolinea la sempre maggiore importanza, anche nel mercato azionario, degli asset intangibili. L'autore sostiene infatti che i capitali immateriali dominano la Borsa, soprattutto in USA. Gli asset intangibili, secondo *Brand Finance*, valgono il 76% di tutto il valore d'impresa delle società quotate in USA, tre quarti *dell'enterprise value* sarebbe infatti costituito da patrimonio diverso da beni fisici o attività finanziarie.

[193] Questa considerazione è sostenuta da F. ROTONDI, *Diritto del lavoro e delle relazioni industriali 2017*, Ipsoa, 2016, 248. In tal senso l'autore aggiunge che le imprese ad alto contenuto tecnologico sono in primo piano per la capacità di ricerca di contenuti distintivi e prodotti tecnologici. Nel caso delle imprese con modello gestionale "tradizionale" l'attenzione invece sarebbe maggiormente posta sui marchi, sulla struttura di distribuzione e sul possesso di tecnologie distintive che accrescerebbero l'efficienza della produzione. Inoltre, il know-how, l'immagine, il portafoglio clienti risulterebbero essere punti di forza delle imprese ad alto contenuto professionale e high tech, attività operanti in settori come la comunicazione, nella finanza, o enti di gestione di patrimoni mobiliari, che, in contrapposizione, hanno un patrimonio tangibile assai più contenuto.

redazione del bilancio dei beni intangibili (si veda *supra* 1.5.), dove si è illustrato come tali capitali debbano essere contabilizzati nel patrimonio dell'impresa. Rimangono, a mio parere, poco comprensibili le ragioni che portano ad una stesura di un bilancio senza una corretta presentazione del valore del capitale intangibile dell'impresa, capitale che, così facendo, rimarrebbe completamente "invisibile" nelle valutazioni oggettive del mercato e dei soggetti esterni all'impresa, sebbene, come già evidenziato, sia ormai riconosciuta la rilevanza dei capitali intangibili ai fini delle attività d'impresa e dei relativi utili. Le imprese spesso prestano molta più attenzione alla corretta iscrizione in bilancio degli asset materiali, mentre assai meno si focalizzano su l'inserimento degli asset intangibili a bilancio, anche se, come indicato poc'anzi, frequentemente questi costituiscano la fonte primaria di redditività e di innovazione.

Molta attenzione dev'essere posta su questo tema, in particolare la redazione del bilancio d'esercizio deve rispondere ai requisiti stabiliti dall'art. 2423 c.c.; se l'impresa non iscrivesse in bilancio le voci relative al capitale intangibile potrebbe esservi un problema di non conformità, in quanto il bilancio non risponderebbe ai principi di rappresentazione veritiera e corretta della situazione economica, patrimoniale e finanziaria dell'impresa come stabilito dall'art. 2423 c.c.[194].

Risulta perciò necessario ridefinire il patrimonio dell'impresa tramite una rivalutazione e un'iscrizione del reale valore delle poste in bilancio inerenti i beni intangibili, e ciò può essere effettuato adeguando la redazione del bilancio alle più moderne metodologie. Il patrimonio dell'impresa potrà acquisire un maggior valore grazie ad una rappresentazione corretta nel bilancio di questi beni di proprietà dell'impresa, come possono essere brevetti, segreti commerciali e marchi. Gli stessi segreti commerciali possono correttamente rientrare nel bilancio d'esercizio dell'impresa, secondo le disposizioni dell'OIC, limitatamente però al solo valore di costo, fatto salvo alcune eccezioni (si veda *supra* 1.5.). Se i segreti fossero correttamente rivalutati nel tempo diventerebbero un asset strategico in grado di incrementare le performance dell'impresa, contribuendo inoltre a sostenere la costituzione di un bilancio

[194] L'art. 2423 c.c. stabilisce che nel caso l'applicazione delle disposizioni degli articoli seguenti, riguardanti la redazione del bilancio d'esercizio, sia incompatibile con la rappresentazione veritiera e corretta, tali disposizioni non dovrebbero venir applicate. In nota integrativa l'impresa deve comunque motivare questa deroga, indicandone l'influenza sulla rappresentazione della situazione patrimoniale, finanziaria e del risultato economico. L'art. 2423 c.c. aggiunge che gli eventuali utili derivanti dalla deroga applicata devono essere iscritti in una riserva non distribuibile, se non in misura corrispondente al possibile valore recuperato. Dev'essere quindi chiaramente valutabile il valore del capitale intangibile perché questo possa e debba essere iscritto nel bilancio d'esercizio. Si veda in tal senso M.S. AVI, (nt. 77), 20 ss.

solido, sia sotto il profilo economico che finanziario. Ciò risulterebbe particolarmente importante per tutte quelle imprese che si ritrovano in uno stato di difficoltà economica, soprattutto in un momento storico come quello attuale, dove le attività economiche presentano forti perdite causate dalla crisi economica innescata con la pandemia.

La stessa UE sostiene l'importanza del capitale intangibile nella creazione di redditività per le imprese. Proprio in tal senso L'EPO e EUIPO hanno analizzato, nel periodo 2011-2013, come le imprese ad alta intensità di diritti di proprietà intellettuale contribuiscano alla formazione del PIL, dell'occupazione e del commercio nell'area comunitaria: dalla ricerca risulta che queste imprese generano il 42% del PIL europeo totale, costituendo il 27,8% di tutti i posti di lavoro nella zona UE, impiegando, tra lavoratori diretti e indotto, un totale di 82,2 milioni di dipendenti (il 38,1% del numero totale dei lavoratori nei Paesi membri). Questi dati dimostrano chiaramente come le imprese ad alta intensità di diritti di proprietà intellettuale hanno un ruolo essenziale nella generazione di produzione e ricchezza nel territorio comunitario e, per di più, i valori indicano che tali imprese sono riuscite ad affrontare meglio la crisi economica del 2008 rispetto all'economia nel suo complesso[195].

Analoga relazione, aggiornata a settembre 2019 e relativa al periodo 2014-2016, individua in Europa circa 353 industrie ad alta intensità di diritti di proprietà intellettuale. Queste imprese, durante il periodo esaminato, hanno generato il 29,2% di tutti i posti di lavoro nell'UE, impegnando mediamente 63 milioni di persone, con 21 milioni di addetti occupati nell'indotto, con un totale di 83,8 milioni di lavori occupati nel settore, il 38,9 % del totale europeo. Sempre nel triennio 2014-2016, le imprese ad alta intensità di diritti di proprietà intellettuale hanno generato circa 6.600 miliardi di euro, contribuendo al 45% del PIL della zona UE. Ancora, queste tipologie di imprese corrispondono salari ai loro dipendenti mediamente più elevati, superiori al 47% rispetto la media europea. Tale aspetto sarebbe favorito dal fatto che l'apporto del valore aggiunto del dipendente nell'impresa ad alta intensità di diritti di proprietà intellettuale è solitamente più elevato rispetto ad altri settori

---

[195] Si veda in tal senso il rapporto in collaborazione tra EPO e EUIPO, *Industrie ad alta intensità di diritti di proprietà intellettuale e risultati economici nell'Unione europea. Rapporto di analisi a livello industriale*, ottobre 2016, reperibile in internet al seguente indirizzo: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/performance_in_the_European_Union/eperformance_in_the_European_Union_sum-it.pdf. Tale studio rappresenta il periodo 2011-2013, mentre il primo aggiornamento del rapporto copriva il periodo 2008-2010, da cui risultava che le industrie d alta intensità di diritti di proprietà intellettuale rappresentavano il 39% della produzione economica dell'UE e il 26% dell'occupazione, nel corso dei due rapporti si è visto dunque un progressivo miglioramento.

dell'economia[196].

In sintesi, confrontando il periodo 2011-2013 con il periodo 2014-2016, si può notare come il contributo alla generazione del PIL europeo da parte delle imprese ad alto contenuto di diritti di proprietà industriale è aumentato nel corso degli anni e, ciò è probabilmente dovuto anche al fatto che tra queste imprese se ne riscontrano numerose attive nello sviluppo di tecnologie per la produzione di energia rinnovabile e attività legate alla quarta rivoluzione industriale.

È inoltre necessario precisare che tale studio non comprende la valutazione delle imprese che fanno uso di segreti commerciali: il segreto commerciale è infatti rientrato all'interno dei beni immateriali solo attraverso il Decreto Legislativo 11 maggio 2018, n. 63, e quindi, successivamente allo studio eseguito dall'EUIPO e qui presentato. Il peso attuale dei beni intangibili nella generazione del PIL totale europeo sarebbe quindi sostanzialmente più elevato rispetto ai dati presentati per il triennio 2014-2016. In studi più recenti, aggiornati a febbraio 2021, le imprese titolari di diritti di proprietà intellettuale conseguirebbero un fatturato per dipendente del 20% superiore rispetto alle imprese che non ne detengono, corrisponderebbero inoltre una retribuzione che è in media del 19% più elevata, confermando perciò le stime di crescita di questa tipologia di imprese[197].

---

196 In tal senso si veda il rapporto di collaborazione tra EPO e EUIPO, *Industrie ad alta intensità di diritti di proprietà intellettuale e risultati economici nell'Unione europea. Analisi a livello industriale*, settembre 2019, terza edizione. Reperibile in internet al seguente indirizzo: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/IPR-intensive_industries_and_economicin_EU/summary/IP_Contribution_Report_092019_execsum_it.pdf. Il Direttore esecutivo dell'EUIPO, Christian Archambeau, si è espresso analizzando lo studio e dichiarando che: "Le industrie che fanno un uso intensivo dei diritti di proprietà intellettuale svolgono un ruolo cruciale nell'accrescere la prosperità dell'UE e nel garantirne il futuro economico. Sono più innovative e hanno una maggiore resilienza di fronte alle crisi economiche. La nostra sfida consiste nel far sì che tutte le aziende e tutti gli imprenditori possano proteggere i loro diritti di Proprietà Intellettuale, in particolare le PMI". Anche il Presidente dell'Ufficio Europeo dei Brevetti, António Campinos, condivide l'importanza del capitale immateriale, affermando che: "L'importanza delle industrie ad alta intensità di diritti di proprietà intellettuale rispecchia la forza dell'economia basata sulla conoscenza in Europa. Le imprese di tali settori spesso proteggono le proprie attività intellettuali attraverso una combinazione di diritti di proprietà intellettuale. Questa strategia crea prodotti e servizi ad alto valore aggiunto, contribuendo in tal modo a garantire la competitività a lungo termine dell'Europa. Alle industrie ad alta intensità di diritti di proprietà intellettuale è riconducibile anche la maggior parte degli scambi commerciali di prodotti e servizi tra l'UE e le altre regioni del mondo (81%). Nel 2016 l'UE nel suo insieme ha registrato un avanzo commerciale complessivo di circa 182 miliardi di euro nelle industrie ad alta intensità di diritti di proprietà intellettuale". Tutte le citazioni sono estrapolate dal testo di E. SALVATORE, (nt. 76), 32.

197 In tal senso si è espresso anche E. SALVATORE, (nt. 76), 35, aggiungendo che i dati illustrati in questi rapporti devono rappresentare un'adeguata chiave di lettura, utile a modificare in ogni suo aspetto il modo attuale di fare impresa. Lo studio EPO-EUIPO "*Industrie ad alta intensità di diritti di proprietà intellettuale e risultati economici nell'Unione europea"* sarà disponibile nel 2022 nella sua ultima versione e tratterà probabilmente il triennio 2017-2019, in base ai report precedenti. Nel testo i dati riportati di febbraio 2021, si riferiscono allo studio di *follow-up*, *I diritti di proprietà intellettuale e la performance delle imprese nell'UE Relazione tecnica a livello di impresa,* EUIPO*,* 2021, reperibile in internet al seguente indirizzo: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/IPContributionStudy/IPR_firm_performance_in_EU/exec/2021_IP_Rights_and_firm_performance_in_the_EU_exec_it.pdf.

4.3. Il legame tra segreto commerciale e settore digitale

Il mercato del settore digitale è fortemente collegato al tema della valorizzazione dei beni intangibili, in quanto pressoché la totalità dei prodotti e dei servizi offerti dal settore digitale si presenta in uno stato immateriale. Da come indicato nella classificazione disposta da Anitec-Assinform (si veda *supra* pg. 85 ss.), solamente una delle quattro macro aree che costituisce il settore digitale è rappresentata da beni materiali: il primo comparto del mercato digitale infatti comprende tutti i dispositivi per la casa e per l'ufficio, quali pc e videogiochi, gli *enterprise e specialized system* come sistemi di *storag*e, server e i *personal e mobile device,* quali *smartphone, tablet, laptop,* tutti prodotti che, insieme alle loro componenti hardware, sono presenti materialmente nelle imprese e non vanno perciò a costituire il capitale intangibile dell'impresa. Le restanti tre macro aree descritte nel rapporto invece, assieme ai *digital enablers,* sono beni presenti in uno stato immateriale nelle imprese e quindi sono valutate come patrimonio e strumenti di carattere intangibile.

Abbiamo già analizzato nel precedente paragrafo come sia il settore digitale che i beni intangibili stiano sempre più acquisendo una centralità nello sviluppo delle attività imprenditoriali generando quella che si può definire un'economia digitale. Diventa perciò di fondamentale importanza, in questo contesto, la protezione di questi capitali intangibili con sistemi che risultino allo stesso tempo sicuri ed efficienti, garantendo perciò la tutela del valore del patrimonio digitale dell'impresa nel tempo.

Tra i vari strumenti a disposizione per la tutela di questo patrimonio sicuramente il segreto commerciale risulta tra quelli più adeguati e performanti, questo per diverse ragione: l'ambito di applicazione della tutela del segreto commerciale è molto ampio e non presenta vincoli particolari, qualsiasi patrimonio, benché risponda ai requisiti previsti dalla legge, può essere infatti tutelato come segreto, quindi questo strumento di tutela si applica perfettamente ad un settore in costante cambiamento, com'è quello digitale, il quale presenta una continua e costante introduzione di innovazioni e lo sviluppo di numerose nuove tecnologie, con campi di applicazione che possono essere fortemente diversificati tra loro[198]. Il segreto commerciale

[198] Per esempio, la società Vodafone, uno dei più grandi *players* mondiali attivi nel settore digitale, ha applicato la tutela del segreto commerciale per la protezione di alcuni suoi documenti contenenti informazioni tecniche e accordi commerciali. Si veda in tal senso la sentenza del T.A.R. della Regione Lombardia, Milano Sez. III, 17 dicembre 2013, n. 2845, in *DeJure*, che ha confermato la sussistenza della tutela di informazioni come segreto commerciale, indicando che: "Vodafone ha negato il suo consenso all'accesso in quanto i documenti contengono dati sensibili (appunto segreti tecnici e commerciali) riguardanti la strategia del Gruppo Vodafone (ad es. accordi di roaming, accordi con i fornitori di hardware, accordi con fornitori di infrastrutture software, protezione di asset e brevetti ed infine protezione di segreti industriali del Gruppo Vodafone)".

ben si adatta a questa situazione, in particolare perché la sua costituzione è immediata e veloce, non necessita di norma di investimenti economici elevati, né di pubblicazione e divulgazione dell'invenzione al pubblico, non sono previsti processi di registrazione presso l'UIBM o presso altri uffici competenti, come è invece previsto per il brevetto. La protezione garantita dall'istituto giuridico del segreto commerciale inoltre è indefinita, e può dunque coprire anche un periodo di lunga durata (finanche perdura), che può essere determinato dal suo titolare a seconda del bisogno e delle strategie, non sono previsti perciò limiti temporali e territoriali, differentemente da quanto disposto invece per altri istituti quali il diritto d'autore e i brevetti[199].

L'Euopean IPR Helpdesk ha descritto quali informazioni, conoscenze e documenti costituiscano i segreti commerciali più apprezzati e utilizzati dalle imprese; tra quelli indicati molti appartengono al settore digitale, come programmi per computer, database, formule e ricette. Tuttavia abbiamo già visto al paragrafo 2.5.2. che nel caso specifico dei software la protezione tramite segreto commerciale può essere applicata solamente ad alcune sue componenti, come il codice sorgente, rispettando contemporaneamente le disposizioni previste per il diritto d'autore, che rimane tuttavia l'istituto giuridico ad oggi espressamente previsto dal legislatore per la tutela dei software*,* mentre possiamo aggiungere che il segreto commerciale gioca un ruolo di rafforzamento o di supporto della tutela contro acquisizioni non legittime[200].

Oltre a ciò, lo stretto legame tra segreto commerciale e settore digitale si rileva nei possibili strumenti di protezione a tutela dell'informazione segreta, in quanto il settore digitale offre molte soluzioni alle imprese. Infatti, tutte le informazioni possibilmente tutelabili come segreti commerciali, quali analisi di mercato, rapporti d'affari, informazioni sui prezzi e costi ecc., possono e sempre più vengono mantenuti in uno stato digitale dalle imprese, ed è quindi necessario prevedere che il mantenimento dell'informazione in uno stato di segretezza sia attuato attraverso delle misure di protezione a loro volta digitali.

La diffusione di processi quali la *digital transformation* e la c.d. *data-driven economy* ha

---

[199] Come indicato nel documento European IPR Helpdesk, (nt. 166), 10. e dal sito ufficiale della Camera di Commercio Milano Monza Brianza Lodi, *Segreto commerciale,* reperibile in internet al seguente indirizzo: https://www.milomb.camcom.it/segreto-industriale.

[200] E' il caso di Google, che ha applicato la tutela del segreto industriale al proprio software e all'algoritmo sotteso che permette l'indicizzazione dei risultati nel motore di ricerca o *ranking* dei risultati. Per una maggiore trattazione del caso si veda *infra* 4.10. Le indicazioni dei tipi di segreti commerciali più apprezzati dalle PMI sono presenti nell'European IPR Helpdesk, (nt. 166), 2.

aumentato progressivamente il quantitativo di dati e di documenti conservati in formato digitale, anziché cartaceo o su altre tipologie di supporti, permettendo modalità di trattamento e di elaborazione dei dati in passato impensabile, generando informazioni di una certa rilevanza economica e suscettibili di ulteriore valorizzazione. Le informazioni digitali presentano però un'estrema mobilità e variabilità dei contenuti, è dunque essenziale prevedere che il processo di digitalizzazione non comporti una riduzione del livello di sicurezza della segretezza di tali informazioni.

La diffusione di conoscenze e di dati in formato digitale ha infatti generato nuove minacce connesse alla sottrazione di dati e informazioni sensibili, facilitando la riproduzione e l'appropriazione indebita dei dati riservati da parte di chi ha una facoltà d'accesso vincolata a obblighi di confidenzialità. Ancora, si possono rilevare rischi connessi all'accesso abusivo tramite attacchi *hacker* a database d'imprese, a siti web o alle piattaforme delle amministrazioni pubbliche. Proprio in tal senso il Legislatore ha previsto, con il nuovo terzo comma dell'art. 623 c.p., un aumento di pena in caso di illecito acquisto, rivelazione o utilizzo di un segreto commerciale tramite strumenti informatici[201].

Ed è proprio su questo particolare aspetto che risulta di primaria importanza il legame che intercorre tra beni intangibili, mercato digitale e segreto commerciale. Sintetizzando, la digitalizzazione ha comportato una sempre maggiore conversione di informazioni riservate in uno stato intangibile, la loro protezione può essere efficacemente garantita dal segreto commerciale attraverso adeguate misure che sono offerte dal mercato digitale. Possiamo quindi concludere che la probabile e attuale crescita dei processi di digitalizzazione delle attività, processo fortemente necessario in Italia visto il ritardo accumulato rispetto agli altri

---

[201] Si veda il nuovo terzo comma dell'art. 623 c.p. in attuazione della direttiva UE 2016/943 in cui si statuisce che: "Se il fatto relativo ai segreti commerciali e` commesso tramite qualsiasi strumento informatico, la pena è aumentata". Si veda anche G. GUALTIERI, (nt. 62), 167 e A. FROLLA, *Cybercrimini, 2020 anno nero: sotto attacco sanità, pagamenti cashless e aziende,* LaRepubblica, 2021. Durante il 2020 si è visto un aumento esponenziale dei reati collegati a furto dei dati, violazione della privacy e perdite di denaro sia nella pubblica amministrazione, che nelle imprese. Come esposto da A. FROLLA il 2020 è stato certamente un *annus horribilis* per l'intero pianeta a causa della pandemia di Covid-19, ma le restrizioni imposte hanno avuto delle ripercussioni anche per ciò che concerne la sicurezza informatica. I criminali informatici hanno infatti sfruttato la situazione creatasi a loro favore, essendoci meno controlli e una platea certamente più grande di possibili dispositivi connessi da attaccare. Ad aumentare progressivamente il rischio connesso a *cybercrimini* sono state la possibile assenza di contromisure adeguate. Secondo l'autore dunque la forbice tra attacco e difesa è stata allargata ulteriormente, e aumenterà in futuro. Nei primi tre trimestri del 2020 si è arrivati infatti a contare 605 attività criminali tra attacchi informatici (450), offensive andate a buon fine (112) e violazioni della privacy (43), con un aumento complessivo dell'86% rispetto ai valori registrati nel 2019. In tutto il 2020, in Italia, oltre il 60% degli eventi criminali ha provocato il furto di dati, superando di gran lunga sia le violazioni della privacy (13% del totale, che risultano comunque quasi triplicate dall'inizio del 2020) che le perdite di denaro (10%). In tal senso si veda anche M. LIBERTINI, *Le informazioni commerciali riservate (segreti commerciali) come oggetto di diritti di proprietà industriale",* in *Dir. ind*., 2017, VI, 566.

paesi UE, parallelamente comporterà un aumento della diffusione degli strumenti di tutela come il segreto commerciale e delle misure digitali adeguate che permettono la costituzione di misure di protezione di tali informazioni.

4.4. Strumenti digitali per la protezione dei segreti industriali

In questo paragrafo si presenteranno gli strumenti digitali che le imprese possono utilizzare per garantire la segretezza delle informazioni preservate in uno stato digitale, strumenti che sono ragionevolmente adeguati a mantenerle segrete, come disposto dal terzo requisito dell'art. 98 c.p.i. per la costituzione di una tutela dell'informazione come segreto commerciale.

È necessario però precisare che non si andrà ad illustrare specificamente le caratteristiche di ogni strumento di protezione digitale, bensì si indicheranno quelle che possono essere le possibili misure attuate dalle organizzazioni per prevenire acquisizioni illecite di informazioni segrete mantenute in uno stato digitale. Data la complessità della materia, si ritiene opportuna, per la composizione di una tutela efficiente del segreto, una collaborazione tra diversi professionisti, in modo da costituire un team interfunzionale che contenga al suo interno un mix di competenze di natura sia giuridico-organizzato che tecnico-informatico.

Illustrando le misure endoaziendali che l'impresa può adottare per la tutela della segretezza delle proprie informazioni, abbiamo già indicato alcuni strumenti che possono venir utilizzati, cui possiamo aggiungere la predisposizione di un sistema di accesso alle informazioni tramite *user name* e password. In giurisprudenza si trovano però diverse valutazioni della validità di questa forma di protezione, si è infatti più volte indicato come la sola applicazione di un sistema di accesso tramite password non possa bastare per ritenere le misure di protezioni adeguate. Come indicato dal Tribunale di Milano, nella sentenza del 14 febbraio 2012: "*Non integra il requisito delle misure idonee a garantire la segretezza delle informazioni necessario alla tutela di cui all'art. 98 c.p.i. l'avere unicamente dotato i dipendenti di una semplice password e login e il non avere adottato misure ulteriori*"[202]. Saranno quindi opportune delle

[202] Nello stesso senso si è espresso il Trib. Venezia con la sentenza del 20 novembre 2009, in *Codice ipertestuale commentato della proprietà industriale ed intellettuale* a cura di C. GALLI, A. GAMBINO, Utet Giuridica, Padova, 2011, 908. Anche la App. di Torino, 28 gennaio 2010, in *DeJure* si è espressa sul livello di tutela offerto da tale misura di protezione, indicando che: "A fini della tutela prevista dall'art. 6-*bis* l.i., non si può ritenere adeguatamente tutelata la riservatezza del contenuto del computer del titolare di un'impresa che, una volta acceso ed attivato tramite una semplice password, resti acceso per l'intera giornata, sia lasciato abbandonato ed incustodito in un ufficio aperto e venga spento da un dipendente incaricato di provvedere a tale incombenza".

misure di protezione accessorie per assicurare la tutela dell'informazione come segreto commerciale, quali, ad esempio, un sistema di tracciabilità degli ingressi ai database o la necessaria autorizzazione per l'accesso alle informazioni da parte del personale responsabile[203]. Si può quindi concludere che la valutazione dell'adeguatezza della citata misura verrà effettuata prendendo in considerazione il caso specifico e che la sola predisposizione di una password d'accesso potrebbe dunque non bastare[204]. Si ritiene in ogni caso necessario e consigliato che la password sia costituita da codici alfa-numerici capaci di garantire un alto livello di sicurezza, non utilizzando parole di uso comune o formule che banalmente potrebbero venir scoperte da terzi esterni all'impresa; inoltre, la password, dovrà essere sottoposta ad una modifica periodica, effettuando così un aggiornamento costante. Per garantire la segretezza della password un'eventuale custodia del codice segreto dovrà garantire un livello di sicurezza adeguato; il codice segreto non dovrà, in ogni caso, essere salvato su documenti o dispositivi esterni, dispositivi che potrebbero venir facilmente rubati annullando la segretezza della password[205].

Per assicurare una difesa contro le minacce informatiche le imprese, titolari di segreti commerciali in formato digitale, dovranno necessariamente installare e mantenere aggiornati su tutti i dispositivi coinvolti software antivirus in grado di costituire e sviluppare difese

---

[203] Come illustrato dal Trib. Milano Sez. Proprietà' Industriale e Intellettuale, 5 luglio 2010 in *Dejure*, in cui si indica che la predisposizione di un sistema di password e un sistema di controllo degli accessi è misura adeguata, indicando infatti che: "Qualora le informazioni siano ad accessibilità controllata e limitata, mediante limiti imposti al personale (*user name* e password) tali da rendere le informazioni protette verso l'esterno e quindi inaccessibili ai terzi, corredate dalla tracciabilità degli accessi ai medesimi, risulta soddisfatto l'ultimo requisito indicato dall'art. 98 c.p.i.". Come indicato anche dal Trib. Torino Sez. spec. Impresa, 15 novembre 2018, n. 5246, in *Dejure*, il sistema di accesso tramite password risulta adeguato, in quanto sono informazioni: "Contenute in banche dati sottoposte a significative misure di protezione: per accedere ai relativi software occorre un account ufficiale aziendale, in cui entrare attraverso un computer abilitato ad operare nella rete interna, a seguito di formale richiesta e autorizzazione da parte del responsabile, a mezzo di password con elevato grado di sicurezza; inoltre sono previste ulteriori limitazioni di accesso, di sola lettura o scrittura, a specifiche aree e database, al fine di compiere determinate operazioni o estrazioni".

[204] Si veda, in tal senso, la sentenza del Trib. Bologna sez. IV, del 27 luglio 2015, n. 2340, in *DeJure*, dove si è analizzato un caso specifico d'insufficienza nell'adeguatezza delle misure di protezione. Il giudice ha ravvisato infatti: "Insufficiente a conferire ai dati aziendali in esame il carattere della segretezza nell'accezione di cui alla lett. c) dell'art. 98 c.p.i., custodire i disegni tecnici in un personal computer privato, dotato di password ed in uso esclusivo al socio-amministratore e coprogettista, misura non adeguatamente protettiva, in quanto, in primo luogo, le informazioni erano state immesse in un computer privato ed in dotazione esclusiva al socio anziché in un sistema informatico aziendale direttamente gestibile e controllabile dalla società, oltre che sull'operato del medesimo e, segnatamente sull'utilizzo dei dati e delle informazioni in questione, non risulta che la società abbia esercitato alcun controllo, dato specifiche direttive o posto limiti atti a prevenirne un uso abusivo".

[205] Si veda in tal senso P. MARINI, *Come costruire un sistema di gestione privacy?,* Utet Giuridica, 2019 100, in cui si indica che nell'allegato B del d. lgs. 196/2003, abrogato poi dall'art. 27, co. 1, lett. d del d. lgs. 10 agosto 2018, n. 101. veniva richiesto un aggiornamento della password una volta ogni 6 mesi, salvo che i trattamenti contenuti concernessero anche dati sensibili e/o giudiziari, nel qual caso il termine si dimezzava a soli 3 mesi. Era ed è comunque considerata opportuna, se del caso, una frequenza maggiore di modifica della password.

contro i più moderni *malware*[206]. In ambito informatico, trattando di antivirus, ci si riferisce spesso anche con il termine "*antimalware*", che è essenzialmente un sinonimo, queste tipologie di software sono destinate alla rilevazione e all'eliminazione di codici malevoli, che se inseriti nel sistema informatico dell'organizzazione possono comportare seri danni e rischi, come permettere a terzi l'acquisizione d'informazioni segrete dall'impresa salvate all'interno dei database o nei dispositivi compromessi. L'attuazione di efficaci misure di protezione tramite *antimalware* potrà perciò limitare minacce di questo tipo, evitando così che i segreti commerciali possano venir illecitamente acquisiti da parte di soggetti definiti come "*criminal hacker*"[207].

Per l'eliminazione dei rischi connessi a particolari *malware* definiti come *spyware* o "file spia", in grado di spiare le attività di un utente, senza che la vittima se ne accorga, *smartphone* e computer devono essere dotati di software di tipo *antyspyware* o schermi definiti "di contrasto" rispetto a clonazioni e furti d'identità. I *spyware* sono particolarmente minacciosi per le attività imprenditoriali in quanto sono capaci di far acquisire informazioni, come segreti commerciali, riguardanti le attività dell'utente, in maniera incognita, senza che la vittima se ne accorga. Tali informazioni vengono poi inoltrarle a soggetti esterni che li utilizzano per trarne profitti economici[208].

Importanti sistemi di salvaguardia della sicurezza della struttura digitale di un'impresa sono i *firewall:* queste componenti, che possono essere sia hardware che software*,* o di entrambe le tipologie, sono necessarie in tutte quelle attività che, utilizzando e sviluppando sistemi informatici, creano connessioni tra più reti, e necessitano dunque di sistemi per preservare il traffico che intercorre tra queste reti. Il *firewall* svolge proprio questa funzione, connettendo e allo stesso tempo monitorando il traffico dei dati tra due o più reti diverse, costituendo una

---

[206] *Malware* è una crasi delle parole "*malicious* software", con questo termine s'include qualunque tipo di software dannoso tra cui i virus, come indicato da G. SBARAGLIA, *Antivirus e antimalware: cosa sono, come funzionano e i 5 migliori da installare subito,* cybersecurity.it, 2019*,* reperibile in internet al seguente indirizzo: https://www.cybersecurity360.it/soluzioni-aziendali/antivirus-e-antimalware-cosa-sono-come-funzionano-come-scegliere-quello-giusto/.

[207] Come indicato da B. PANATTONI, (nt. 170), 60. Illustrando gli strumenti di sicurezza più volte B. PANATTONI si riferisce alla necessità per le imprese di prevedere sistemi di protezione tramite antivirus, evidenziando che per una tutela efficace delle informazioni l'impresa dovrebbe dotare a tutti i dispositivi che lo consentono di software di protezione (come di antivirus, *antimalware* ecc.) regolarmente aggiornati. In tal modo sia le reti che i sistemi informatici sarebbero protetti da accessi non autorizzati attraverso strumenti specifici, come *firewall* e altri dispositivi/software antintrusione, istallando e mantenendo sempre aggiornato il software.

[208] Anche il T.A.R. Palermo, sez. II, 26 giugno 2012, n.1300 in *DeJure*, cita gli *antyspyware* come misure atte a prevenire, contenere ed evitare i rischi connessi dall'acquisizione illecita di informazione effettuato attraverso l'utilizzo di file spia.

barriera tra le reti interne, che possono essere più sicure e controllate, e le reti esterne, che invece possono essere meno affidabili, come nel caso della rete internet. Ciò solitamente viene eseguito tramite un sistema di *policy* e di regole imposte dal *firewall,* che è così in grado di determinare quale traffico può transitare tra una rete e l'altra e quale invece dev'essere bloccato per motivi di sicurezza o in quanto contenente dei possibili elementi rischiosi per le reti stesse[209].

Per aumentare ulteriormente il livello di sicurezza e costituire un sostanziale monitoraggio degli accessi l'impresa potrebbe prevedere lo sviluppo di un sistema di autenticazione, sistema capace di controllare l'identità virtuale dei soggetti che accedono alle banche dati, ai database e a tutte quelle informazioni considerate riservate o segrete dall'impresa. Il sistema di autenticazione può essere costituito da accessi controllati, effettuabili solamente con la predisposizione di *user name* e password, si può, in aggiunta, approntare un secondo elemento di autenticazione, come attraverso la definizione di una parola chiave. Altri sistemi più sofisticati possono richiedere l'inserimento di elementi biologici (come riconoscimento dell'iride, impronte digitali, impronte vocali, riconoscimento del volto e altro ancora) o attraverso un particolare oggetto (tessera magnetica, *smart card*, usb token, etc.): tutte queste misure sono in grado di aumentare ulteriormente il livello di protezione delle informazioni e andranno costituite in base al livello di importanza e di segretezza dell'informazione[210].

La protezione di documenti e di dati sensibili contenenti segreti commerciali può essere assicurata anche da metodi di sicurezza come la crittografia. Questi sistemi prevedono la scrittura del contenuto delle informazioni in un formato nascosto, in un modo tale da apparire

---

[209] Come indicato nel sito ufficiale di Cisco, multinazionale americana specializzata nella fornitura di apparati di *networking*, alla pagina *Cos'è un firewall?*, n.d., i sistemi di protezione *firewall* sono citati dalla Cassazione penale sez. V, 06 giugno 2007, n. 31135, in *DeJure*, come mezzi volti a garantire l'accesso di estranei alle informazioni dell'impresa, specificando che: "Fraudolenta è l'intercettazione non quando sia impossibile o estremamente difficile identificarne l'autore, bensì quando nell'attuarla ci si avvalga di mezzi atti ad eludere i meccanismi di sicurezza volti a impedire l'accesso di estranei alle comunicazioni (password, *firewall*, criptazione od altri analoghi strumenti)". Tratta dei sistemi *firewall* anche B. PANATTONI, (nt. 170), elencando le forme di sicurezza per operare nel *cyberspace.* L'autrice evidenzia che è necessaria una particolare attenzione alla sicurezza nelle comunicazioni e informazioni veicolanti attraverso la rete internet. Le imprese devono prevedere una sezione dedicata alla *network security*, come diversi *firewall*, o procedure di crittografia delle informazioni, ma soprattutto all'interno della *policy* aziendali devono venir determinate le particolari minacce propriamente definite come "*cyber"* e quindi legate ad un corretto e buon utilizzo dei strumenti nel *cyberspace*, formando i propri dipendenti ad un uso attento, consapevole e accorto di tutti gli strumenti e i servizi online.

[210] In tal senso si vedano G. CASSANO, G. VACIAGO e G. SCORZA, *Diritto dell'internet,* Cedam, 2012, 150, in cui, presentando i sistemi di autenticazione, si definiscono questi come strumenti idonei a controllale l'identità virtuale degli accessi. L'identità virtuale è definita come l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore. Il rischio che corre l'impresa non sviluppando sistemi di autenticazioni efficienti è di essere vittima di possibili furti d'identità, tant'è che spesso in letteratura e in dottrina si fa riferimento all'identità digitale proprio per casi di "furto di identità".

illeggibile e inutilizzabile a persone non autorizzate. Bisogna sottolineare che oltre a proteggere le informazioni da possibili acquisizioni illecite, la crittografia rende particolarmente più complesso il processo di *reverse engineering,* che ricordiamo essere uno dei metodi consentiti dalla legge per un'acquisizione lecita di segreti commerciali. Proprio a questo riguardo la crittografia della documentazione risulta specialmente indicata come forma di tutela dei segreti commerciali dell'impresa. Altre tecniche di crittografia possono invece garantire l'autenticità di messaggi o di documenti, come la firma digitale, tecniche capaci di verificare e attestare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici[211].

Non propriamente un sistema di difesa ma più una metodologia atta a recuperare le informazioni perse o danneggiate in caso di *disaster recovery* è il processo di *backup* periodico delle informazioni e dei dati critici che l'impresa può effettuare tramite copie dei dati periodiche su dispositivi esterni, in modo da evitare possibili perdite complete di dati o informazioni. Il *backup* permette di conservare le informazioni nel tempo, dev'essere però predisposto un sistema di salvataggio sicuro e aggiornato, sarà dunque necessario effettuare il processo regolarmente e monitorare che le informazioni siano salvate in allocazioni che garantiscano la loro protezione senza precludere lo stato di segretezza dell'informazione[212].

Infine l'impresa dovrà prevedere che tutti i dispositivi e gli strumenti utilizzati dagli utenti dispongano delle misure di sicurezza atte a limitare il rischio di acquisizione illecita d'informazioni digitali; non solo pc o server dunque, ma anche *smartphones* o *tablet,* o un qualsiasi altro dispositivo connesso al sistema dovrà essere adeguatamente fornito delle protezioni necessarie, così che l'impresa non presenti "punti di debolezza" nel suo sistema informatico.

In questo capitolo si è voluto solo brevemente presentare alcune delle principali misure che le imprese possono sviluppare per tutelare adeguatamente i propri segreti commerciali in

---

[211] In materia App. Torino, sez. spec. in materia di imprese, 19 maggio 2017, in *Pluris:* ivi, la mancanza di misure di crittografia ha comportato il diniego alla parte attrice della facoltà di godere della protezione delle proprie informazioni come segreto commerciale, in quanto, come indicato del giudice: "I file SI, lungi dall'essere in qualche modo criptati, sono facilmente accessibili ed analizzabili da chiunque; l'attrice per ottenere l'impenetrabilità avrebbe potuto utilizzare tecniche volte all'offuscamento, quali la crittografia, che non si rinvengono nel caso di specie, non sussiste alcuna violazione del segreto, come stabilito agli artt. 98 e 99 c.p.i., da parte delle convenute, che non hanno replicato il codice sorgente dei file SI ma, attraverso un'attività non complessa per un esperto del settore e lecita, il *reverse engineering*, hanno reso possibile l'importazione dei file formato SI per gli utilizzatori del software". Si veda anche la *Guida alla Firma Digitale,* Centro Nazionale per l'informatica nella pubblica amministrazione, 2009, 10.

[212] Come indicato da B. PANATTONI, (nt. 170), 54.

formato digitale, tuttavia la tecnologia e la materia presenta numerosi altri sistemi che possono essere attuati; inoltre, molto probabilmente, lo sviluppo di altre e più moderne tecnologie e innovazioni in futuro permetteranno nuove e più performanti forme di protezione delle informazioni di quelle attualmente utilizzabili, perciò è necessario che le imprese monitorino costantemente lo "stato" tecnologico delle proprie misure di protezione, perché non risultino obsolete e quindi inefficienti[213].

4.4.1. *Blockchain* come sistema di tutela delle informazioni riservate

Le misure di protezione indicate nel precedente paragrafo possono venir configurate tra loro per costituire un'adeguata tutela dei segreti commerciali conservati in formato digitale. Si è già indicato come il Tribunale, nel determinare la possibilità di applicare la tutela come segreto commerciale e una sua potenziale violazione, verificherà che l'informazione in esame e le misure di protezione ad essa applicate soddisfino tutti i requisiti stabili dall'art. 98 c.p.i. L'impresa titolare dell'informazione potenzialmente tutelabile dovrà dunque presentare al Tribunale competente: una descrizione del segreto commerciale, per verificare l'adempimento a tutti i requisiti minimi, un documento che certifichi cronologicamente il momento della creazione, al fine di determinare la creazione e/o esistenza del segreto e la sua proprietà, e la garanzia che tale informazione sia stata tenuta segreta dal suo detentore. Nel caso di violazione di un segreto commerciale il giudice potrebbe dunque negare la possibilità di applicare la tutela all'informazione se non fossero fornite tutte queste prove. Le imprese necessitano quindi di sistemi che consentano di allegare e provare puntualmente tutti questi elementi inerenti alle informazioni segrete che formano il know-how sviluppato nell'ambito dell'attività imprenditoriale[214].

Dato quanto appena illustrato, molte imprese, oggi, tendono a preferire la conservazione dei propri segreti in un formato materiale, ad esempio presso banche o casseforti domestiche, essendo esse forme di tutela perfettamente conformi alle disposizioni della legge, dove inoltre l'origine cronologica e la validità della tutela dei documenti materiali può venir garantita dal

---

[213] Solo per citare altri sistemi informatici di protezione che le imprese possono sviluppare: *Mandatory Access Control* (MAC), *Intrusion detection system* (IDS), *Network Intrusion Detection System* (NIDS), *Honeypot, Patching.*

[214] In tal senso si veda A. BALBO, *Segreti commerciali: la Blockchain è una "misura ragionevole" per mantenerli al sicuro?,* Cyberlaws, 2018, reperibile in internet al seguente indirizzo: https://www.cyberlaws.it/en/2018/blockchain-segreti-commerciali/.

sistema notarile, superando quindi quel limite che può essere invece riscontrato per i segreti mantenuti in formato digitale, che più difficilmente possono venir autenticati da soggetti o autorità pubbliche. Lo strumento notarile rappresenta infatti un sistema tradizionalmente sicuro, ancorché oneroso, per i detentori di segreti commerciali, al fine di assicurare la tutela dei propri asset strategici durante un processo.

Tuttavia questi limiti riscontrati nei segreti commerciali preservati in formato digitale possono essere efficacemente superati attraverso l'utilizzo delle potenzialità offerte della tecnologia *blockchain*: la notorietà di questa tecnologia è in forte crescita, non solo nel settore che normalmente gli viene ricollegato, cioè nel settore finanziario, grazie all'esplosione del sistema delle criptovalute, ma anche tra imprese e professionisti, i quali necessitano di strumenti per la certificazione e la tutela di documenti, idee, prove d'uso e del loro know-how, dunque in materia di proprietà industriale e intellettuale, nonché nell'ambito di circolazione dei titoli e delle partecipazioni sociali[215].

La tecnologia *blockchain* nasce nel 2008 da un autore la cui identità è ancora ad oggi misteriosa, identificato dietro lo pseudonimo di Satoshi Nakamoto, il quale, pubblicando un articolo tecnico in cui si descriveva un sistema per la contabilizzazione di *commodities* digitali trasferibili chiamati Bitcoin, introduceva per la prima volta al mondo il sistema *blockchain*[216]. Questo sistema si distingueva dai metodi allora esistenti in quanto consentiva ad utenti non identificati di scambiare oggetti in modo sicuro, non censurabile, senza ricorrere ad intermediari fidati e "centrali". Nel 2009 l'idea viene implementata con un software e caricata in rete, dando così vita ad una comunità di utenti, inizialmente di esigue dimensioni, per i quali il principale utilizzato era costituito dallo scambio di valore[217].

Precisando brevemente il funzionamento del sistema *blockchain*, questa può essere descritta come un insieme di tecnologie basate su un registro (in inglese *ledger*) strutturato come una

---

[215] Come indicato anche nell'articolo di D. AQUARO, *Marchi, brevetti e opere: così la blockchain difende la proprietà intellettuale,* IlSole24Ore, 2019. In tal senso si è espressa anche V. MOSCON, *Tecnologie blockchain e gestione digitale del diritto d'autore e connessi,* in *Dir. ind*., 2020, II, 137, sottolineando come in campo accademico, negli ultimi anni, sono state formulate varie ipotesi e suggerimenti in merito a come la tecnologia *blockchain* possa venir utilizzata per la gestione dei diritti d'autore e di altri diritti connessi.

[216] In tal senso si rimanda a NYUMBAYIRE, *Il Consenso di Nakamoto*, in Interlogica, 2017. L'articolo tecnico di S. NAKAMOTO menzionato nel testo è: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Si veda anche F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della Blockchain, Intelligenza Artificiale e IoT,* Milano, Ipsoa, 2018, 9 ss.

[217] Si veda in tal senso F. BRUSCHI, in *Le applicazioni delle nuove tecnologie: criptovalute, blockchain e smart contract,* in *Dir. ind*., 2020, 162 ss.

catena (*chain*) di blocchi (*block*) contenenti delle transazioni in un *network* tra pari (*peer to peer* o P2P), ovvero una rete in cui ogni dispositivo collegato è sia un *client* che un *server.* Con questo sistema gli utenti possono sia condividere che fruire di informazioni con gli altri utenti presenti nella rete sulla base di un rapporto di fiducia che si instaura tra loro, eliminando la presenza di un ente centrale, il quale opererebbe quale validatore delle varie transazioni. Non è richiesto infatti che gli utenti coinvolti (o "nodi") siano a conoscenza dell'identità reciproca, dato che la coerenza tra le varie copie è regolata da un protocollo specifico e dall'aggiunta di un nuovo blocco. Nel sistema *blockchain* ci sono inoltre dei *peer,* chiamati *miner* o "minatori"*,* che raccolgono e organizzano le transazioni in una struttura di dati, che viene appunto chiamata blocco. Ogni blocco è dotato di un "*header*"*,* che contiene a sua volta un codice unico, chiamato *hash,* e il codice *hash* del blocco precedente. In questo modo ciascun blocco è collegato al blocco precedente attraverso i codici *hash* (da cui il nome *blockchain,* traducibile quindi come "catena di blocchi"), definendo l'ordinamento dei blocchi nella catena in maniera cronologica.

In termini riassuntivi la *blockchain* è come una sorta di database distribuito (ed infatti rientra nella categoria delle Distributed Ledger Techonology - DLT) in cui tutti i partecipanti possono operare allo stesso livello. Tale sistema presenta alcune caratteristiche specifiche e un costante monitoraggio dell'autenticità dei contenuti condivisi. La *blockchain* è perciò un sistema d'immagazzinamento di contenuti dove i dati sono conservati in un registro immodificabile e ineliminabile, che permette la tracciabilità e la verifica costante di ogni transazione e un alto livello di sicurezza; questo è garantito dall'uso di tecniche crittografiche: tutte le operazioni effettuate all'interno della *blockchain,* come creazione, modifica o cancellazione di dati, vengono infatti registrate e attribuite ad una specifica identità virtuale, che dev'essere in ogni caso verificata e autorizzata[218].

Il sistema procede dunque con una serie di transizioni crittografate, all'utilizzatore vengono fornite sia una chiave pubblica che una chiave privata: la chiave privata viene utilizzata per firmare le transazione, mentre la chiave pubblica indica l'indirizzo del sistema. In questo

---

[218] La funzione dell'*hash* consente di ridurre un insieme di bit in una stringa alfanumerica, univocamente riconducibile al contenuto originario tramite "un'impronta digitale", come indicato da F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 13. Per una maggiore descrizione del funzionamento della tecnologia *blockchain* si veda R. MORRIELLO, *Blockchain, intelligenza artificiale e internet delle cose in biblioteca,* AIB studi, 2019, 47. Si veda anche l'opera di M. CONOSCENTI, A. VETRO', J.C. DE MARTIN, in *Blockchain for the internet of things: a systematic literature review,* in *2016 IEEE/ACS 13th International conference of computer systems and applications (AICCSA),* New York, IEEE, 2016, in cui si definisce la *blockchain* come un sistema che garantisce privacy, robustezza e assenza di qualsiasi punto debole.

modo l'utilizzatore non dovrà necessariamente usare l'identità della vita reale ma basterà uno pseudonimo, che non è tracciabile né riconducibile all'identità reale, ma non è neanche ricollegabile all'indirizzo IP del proprio computer.

Per quanto concerne la sicurezza, come già indicato poc'anzi, nei sistemi *blockchain* la validazione e la conservazione dei dati non è eseguita da un singolo ente centrale ma da tutti i computer (e quindi i nodi) connessi alla rete che partecipano congiuntamente alla verifica delle transazioni, trasmettendo i nuovi blocchi alla *blockchain* e conservando una copia aggiornata di tutti i registri; maggiore sarà il numero di nodi, più il sistema diventerà sicuro. Sono stati registrati alcuni attacchi informatici al sistema *blockchain* da parte di *miners* poco onesti, possessori di un gran quantitativo di nodi e quindi in grado di esercitare un certo potere sulla catena, in modo tale da cancellare l'anonimato della *blockchain* e rivelare le vere identità degli utilizzatori o i loro indirizzi IP. Tuttavia, al momento, si ritengono questi degli episodi sporadici: la rete è giudicata stabile e sicura, al punto tale che la *blockchain* è già uno standard ISO (ISO TC/307), ed inoltre si stanno comunque cercando altre soluzioni sperimentali per alzare ulteriormente il livello di sicurezza del sistema[219].

Le potenzialità offerte dalla tecnologia *blockchain* alle imprese sono molteplici: oltre ai vantaggi già illustrati, altri sono legati al fatto che si tratta di un'infrastruttura informatica già pronta e operativa che non necessita di dover organizzare la gestione o l'implementazione, consentendo alle imprese di fruirne facilmente, sostenendo degli investimenti contenuti dato che ogni operazione sulla *blockchain* è soggetta ad una piccola commissione espressa in criptovalute[220].

---

[219] Si veda in tal senso R. MORRIELLO, (nt. 218), 48. Si veda la certificazione *blockchain:* ISO TC/307 *Blockchain and distributed ledger technologies,* Geneva, ISO, 2016, reperibile in internet al seguente indirizzo: https://www.iso.org/committee/6266604.html e anche il documento di output di I-Com, Istituto per la Competitività, *Blockchain tra opportunità e sfide,* https://www.i-com.it/wp-content/uploads/2019/11/Blockchain-tra-opportunita-e-sfide.pdf.

[220] Per ciò che concerne il tema delle criptovalute e il suo inquadramento giuridico si veda la sentenza del T.A.R. di Roma sez. II, 27 gennaio 2020, n.1077, in M.M. CONSIGLIA, *Nuova definizione di valute virtuali: l'orientamento del TAR,* in Giustiziacivile.com, 2020, reperibile in internet al seguente indirizzo: https://giustiziacivile.com/banca-finanza-assicurazioni/note/nuova-definizione-di-valute-virtuali-lorientamento-del-tar. Commentando tale sentenza del T.A.R, si indica che le valute virtuali, come le criptovalute, vanno qualificate come "beni" immateriali, giacché da un lato non svolgono le funzioni tipiche della moneta, per via della loro estrema volatilità, e inoltre mancano del potere liberatorio nei pagamenti. Qualificare le valute virtuali come un bene giuridico, disciplinato all'art. 810 c.c., significherebbe considerarle come un bene mobile immateriale, composto da una componente immateriale, ossia dalla stringa alfanumerica registrata sulla blockchain, e da una componente fisica, il supporto materiale in cui viene memorizzato il portafoglio digitale: entrambe sarebbero necessarie a consentirne l'uso come mezzo di pagamento nell'ambito di una transazione. In quest'ottica, l'adempimento di un'obbligazione realizzato tramite valuta virtuale andrebbe qualificato come esecuzione di un contratto di permuta, come disposto all'art. 1552 c.c., ovvero come una prestazione in luogo dell'adempimento, disciplinato all'art. 1197 c.c., ove si ritenga che il prezzo possa essere denominato solo in moneta legale.

L'archiviazione dei dati all'interno della *blockchain* può avvenire tramite un lungo elenco di transazioni, o di come vengono definiti dagli utenti, di "bonifici", effettuati fra i diversi utenti del sistema, all'interno di ogni bonifico va indicata una "causale", che può indicare una qualsiasi informazione, seppur in ridotte dimensione. La registrazione di questa informazione prende il nome di "notarizzazione". Con questo meccanismo viene data all'informazione un "timbro" virtuale temporale che ne accerta la data e l'orario del turno di registrazione. Ed è questo un'importante ulteriore vantaggio della tecnologia *blockchain*, dato che in questa maniera è possibile ottenere una prova documentata che attesti l'esistenza e l'origine cronologica dell'informazione, elementi che abbiamo già discusso poter venir richiesti dal giudice nelle fasi di valutazione dell'adeguatezza ai requisiti stabiliti dalla legge per l'applicazione della tutela all'informazione come segreto commerciale, ovviando perciò a quel problema che era stato evidenziato per le informazioni conservate in formato digitale[221].

Trattando di costi, è necessario evidenziare che, indipendentemente dalla tipologia d'informazione trasferita, la commissione richiesta per la registrazione dell'informazione all'interno della *blockchain* risulta essere molto più economica rispetto al costo dei tradizionali metodi di transazione. Tuttavia, non è facile calcolare l'importo dovuto, in quanto il totale è correlato a diverse variabili, quali il tempo di esecuzione della transazione, il peso del dato caricato, ma soprattutto il valore di mercato del Bitcoin o di altre criptovalute, che sono soggette ad una forte volatilità[222].

Analizzando specificamente il rapporto tra questa tecnologia e l'istituto del segreto commerciale, i documenti elettronici contenenti informazioni segrete possono essere "depositati" in uno dei blocchi che costituisce la *blockchain.* Come indicato precedentemente*,* uno dei vantaggi di questo sistema è che può essere facilmente utilizzato dalle imprese come

---

221 Come illustrato nell'articolo di D. AQUARO, *Blockchain, una tutela in cerca d'autore,* IlSole24Ore, 2019, 21, questo servizio di "notarizzazione" dell'esistenza e dell'origine cronologica dell'informazione non ha nulla a che vedere con i notai. Come indicato da D. AQUARO, però sul tema della proprietà intellettuale il notariato si era mosso, studiando la possibilità di una blockchain notarile, ma: "Quel progetto di Notarchain è stato abbandonato, perché ipotizzava una catena chiusa e non aveva logica un registro delle opere dell'ingegno accessibile ai soli notai", spiega Giampaolo Marcoz, vicepresidente del consiglio nazionale del notariato, il quale precisa ulteriormente che: "Nelle blockchain chiuse, *permissioned*, si può immaginare un ruolo dei notai solo se gli altri nodi sono certificati, istituzionali, e tutti indipendenti. Mentre nelle catene *permissionless* e pubbliche, come Bitcoin, il notaio può agire soltanto *off-chain*, ad esempio come garante dei wallet digitali".

222 Per visualizzare la commissione più adatta alla registrazione e i relativi costi in tempo reale si veda il sito: https://bitcoinfees.earn.com/. Si tenga presente che nel febbraio 2019, per la *blockchain* del Bitcoin la commissione ammontava a circa 0,15 euro per bonifico, ovvero per inserire un'informazione di circa 80 caratteri (lunga la metà di un messaggio SMS) come indicato da O. VENIER, *Intelligenza Artificiale, Blockchain e mondo IoT: l'esperienza degli operatori,* in *Dir. ind*., 2020, II, 170. Va anche detto però che, il valore del Bitcoin nel 2019 era di circa 7.000€, mentre ad oggi (08/04/21) è di circa 48.000€.

prova dell'esistenza e della proprietà di un'informazione tutelabile come segreto commerciale nel corso di un processo attraverso il procedimento di notarizzazione. Esistono già oggi dei servizi che si propongono di notarizzare certe tipologie di documenti attraverso la *blockchain,* favorendo un mantenimento sicuro e garantendo al titolare di poter così provare l'originalità degli stessi[223].

Perché la conservazione del segreto attraverso *blockchain* sia valida, i documenti depositati devono essere noti solamente all'utente titolare del segreto, devono essere inoltre inaccessibili e immodificabili dagli altri utenti della rete, e dagli stessi gestori della rete. Tutti questi aspetti sono rispettati nel sistema *blockchain*: il requisito essenziale della segretezza non è compromesso, considerato che quando si registrano informazioni sulla *blockchain,* le uniche pubblicamente disponibili a tutti gli utenti sono il codice *hash* e il *timestamp,* in cui si indica solamente quando si è verificata la registrazione sulla *blockchain,* ed inoltre al contenuto del blocco può accedere solamente l'utente che lo ha depositato attraverso una *key* da lui selezionata (si ricorda anche che il sistema *blockchain* è costruito da un registro immodificabile e non eliminabile*,* il quale permette la piena tracciabilità e la verifica costante di ogni transizione)[224].

---

223 Si registrano la nascita di alcune start-up, come l'italiana Creativitysafe o la tedesca Bernstein, specializzate in piattaforme di *blockchain.* Queste imprese sono in grado di offrire ai titolari di segreti commerciali servizi di caricamento di un'impronta digitale (cioè una copia del documento) contenente segreti commerciali sulla *blockchain,* rilasciando al suo titolare un certificato, indicante la titolarità e la data di caricamento di tale documento, documento non accessibile dal servizio di caricamento, ma neanche da altri terzi in qualsiasi momento. Come indicato nell'articolo di M. MAGGIORE, M. REGUZZONI, *Segreti industriali, know-how e blockchain,* Creativitysafe.com, reperibile in internet al seguente indirizzo: https://creativitysafe.com/segreti-industriali-know-how-e-blockchain/, la blockchain e le imprese come CreativitySafe offrirebbero uno strumento comodo ed efficace per far valere i diritti afferenti alle informazioni segrete contro dipendenti e terzi concorrenti sleali.

224 Si veda M. MAGGIORE, M. REGUZZONI, (nt. 223) e F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 139, in cui si indica che la funzione di notarizzazione della *blockchain* potrebbe venir applicata anche per una tutela efficace dei brevetti e di altri diritti di proprietà intellettuale. L'Università di Cagliari, in collaborazione con la società spin-off dell'ateneo FlossLab S.r.l. ha sviluppato un sistema di notarizzazione della documentazione: l'Università ha così annunciato, a luglio 2018, che i certificati di laurea verranno rilasciati su *blockchain.* Per un approfondimento sul funzionamento del sistema di pubblicazione dell'informazione tramite *blockchain* si veda O. VENIER, (nt. 222), 170 ss. L'elaborazione del codice alfanumerico che genera l'impronta digitale non potrà mai essere manipolato, in quanto non esiste attualmente un metodo o sistema matematico in grado di manipolare un dato digitale di partenza così da ottenerne un'impronta digitale a piacere. Come indicato da O. VENIER, questo sistema si basa dunque su delle proprietà matematiche che ci permettono di affermare che se disponiamo di un'impronta digitale reale di un qualsiasi file, possiamo parimenti affermare di disporre anche del file corrispondente, questo perché l'impronta potrebbe anche venir inventata, ma non potrebbe a posteriori essere fatta corrispondere ad alcun file reale. Per ciò che concerne le chiavi crittografiche, lo stesso O. VENIER, (nt. 222), 170 ss. aggiunge che le password non rappresenta, come nei sistemi informatici tradizionali, l'accesso ad un servizio, ma costituisce la vera e propria "chiave" di sblocco delle operazioni crittografiche come bonifici, notarizzazioni, scambi di token, ecc. La *blockchain* infatti, non essendo un sistema "centralizzato" non dispone di un sito centrale dove svolgere operazioni come "creare un account" o "recuperare una password persa", oppure di altre operazioni ordinarie presenti nei sistemi centralizzati come *l'home banking*, mentre nella *blockchain* tutte le operazioni sono svolte direttamente tramite le chiavi crittografiche.

Dato che esistono diverse tipologie di reti *blockchain,* è necessario specificare che si ritengono più indicate per una corretta tutela dei segreti commerciali le reti *blockchain* di tipo pubblico (o c.d. *permissionless,* come Bitcoin e Ethereum) in quanto queste risultano essere reti di più grande dimensione e maggiormente incorruttibili; esse sono inoltre reti tendenzialmente sempre accessibili, disponibili a chiunque, senza restrizioni particolari circa la lettura delle transazioni o il compimento delle stesse, e la gestione dei blocchi è affidata ad una platea indefinita di utenti[225]. Per ciò che concerne invece le *blockchain* di tipo *permissioned* (o private), reti chiuse in cui solo alcuni nodi possono approvare e aggiungere nuovi blocchi, queste sarebbero state implementate da alcune società private con l'obiettivo di mantenere una forma di pieno controllo sui partecipanti alla rete stessa. Nelle *blockchain permissioned* possono infatti essere richieste autorizzazioni preventive per l'accesso, si può inoltre decidere a quali utenti del *network* spetti il potere decisionale, con la possibilità di introdurre limitazioni specifiche alla capacità di leggere i contenuti registrati (di qualsiasi natura essi siano), e quindi, limitare l'accesso a documenti contenenti segreti commerciali[226].
Le *blockchain permissioned* risultano meno adatte alla conservazione di segreti commerciali, questo per diversi motivi: la loro costituzione e il loro utilizzo richiedono investimenti economici molto superiori a quelli richiesti per l'impiego di reti *blockchain permissionless,* per garantire la sicurezza e la stabilità del sistema servirebbero numerosi blocchi, tenendo però conto che un solo blocco potrebbe conservare anche molteplici documenti contenenti segreti commerciali. Di conseguenza, perché il sistema risulti funzionale, l'impresa (o il consorzio di imprese) deve possedere diversi e consistenti segreti commerciali da tutelare, altrimenti il rischio è quello di costituire una catena troppo limitata, con pochi blocchi, che non garantirebbe una piena sicurezza del contenuto. Infine, ricordiamo che la gestione della *blockchain permissioned* è affidata a soggetti pre-designati, e ciò risulterebbe non ottimale per la conservazione di segreti commerciali, in quanto gli stessi gestori sarebbero in grado di appropriarsi, modificare o cancellare il contenuto dei blocchi e quindi il segreto

---

225 Per un approfondimento delle diverse tipologie di *blockchain* e le loro caratteristiche si veda F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 21.

226 Si veda in tal senso M. MAUGERI, *Smart contracts e disciplina dei contratti,* in *ODCC,* 2020, II, 378. Si veda anche A. D'ANNA, *La formazione del consenso nella blockchain in assenza di autorità centralizzate, il problema dei generali bizantini e prospettive future,* Cyberlaws, 2020, reperibile in internet al seguente indirizzo: https://www.cyberlaws.it/en/2020/formazione-consenso-blockchain-prospettive-future/.

commerciale[227].

Se dunque le reti *blockchain permissionless* sembrano maggiormente idonee all'archiviazione di documenti contenenti segreti commerciali, è necessario che le imprese sostengano il loro mantenimento, in un processo che si potrebbe definire di "fidelizzazione", anche in un'ottica di sicurezza delle transazioni, che aumenterebbe con una maggiore diffusione della piattaforma. Il solo scopo di *storage* dei segreti commerciali sulla *blockchain* potrebbe però scoraggiare il mantenimento della catena stessa, poiché esistono anche altri strumenti digitali adatti al mantenimento e alla conservazione di informazioni segrete che possono risultare maggiormente agevoli e accessibili rispetto al sistema *blockchain*.

Un'interessante opportunità legata alle *blockchain* di tipo *permissionless,* che favorirebbe l'utilizzo e il mantenimento della catena da parte delle imprese per effettuare operazioni di scambio, potrebbe essere offerto dal processo di tokenizzazione dei segreti commerciali. Definendo brevemente il funzionamento di tale processo, questo si baserebbe su c.d. token, che possono venir categorizzati come "gettoni digitali" contenenti un insieme di informazioni registrate in una *blockchain,* capaci di conferire un certo diritto di proprietà a un determinato soggetto[228]. Il processo di tokenizzazione realizzerebbe dunque la conversione dei diritti su di un bene (materiale e immateriale) in un token digitale registrato su una certa *blockchain*, dove il bene e il token sono collegati tra loro da uno *smart contract,* che nei DLT, come la *blockchain,* è costituito da un programma per elaboratore con funzioni del tipo "*if this then that*", la cui esecuzione vincola automaticamente due o più parti sulla base di condizioni pre-impostate. Gli *smart contracts* potrebbero essere dunque utilizzati per determinare le modalità di fruizione dei contenuti, dando diretta esecuzione agli accordi contrattuali. Sebbene il concetto di *smart contract* esista da tempo, essendo stato teorizzato per la prima volta agli inizi degli anni 90' dall'informatico Nick Szabo (ben prima quindi degli DLT), nel sistema *blockchain* esso ha trovato un'applicazione ideale, data la possibilità di rendere il programma

---

[227] Si veda in tal senso D. AQUARO, in (nt. 221), 20 e D. AQUARO, *Smart contract, la clausola si autoesegue*, IlSole24Ore, 2019, 10, in cui il direttore dell'Osservatorio *blockchain* del Politecnico di Milano, Francesco Bruschi, indica che il successo di una *blockchain* pubblica e aperta come Ethereum, seconda per capitalizzazione dopo Bitcoin, sarebbe proprio dovuto alla sicurezza delle transazioni, che aumenterebbe al grado di diffusione della stessa piattaforma.

[228] Si veda in tal senso anche G. GITTI, M. MAUGERI, C. FERRARI, *Offerte iniziali e scambi di cripto-attività,* in *ODCC*, 2019, I, 97, dove si descrive il token come un gettone virtuale con funzioni di "rappresentazione" di rapporti giuridici. I token si suddividerebbero in tre principali categorie: i token di pagamento, ossia le criptovalute; gli *utility* token, ossia token che permettono di accedere a un'utilizzazione o a un servizio digitale su *blockchain*; e i token d'investimento, o *asset* token, che rappresentano un credito ai sensi del diritto delle obbligazioni nei confronti dell'emittente oppure un diritto sociale ai sensi del diritto societario.

automatico, trasparente e sicuro[229].

Con il processo di tokenizzazione, tramite un'*initial coin offering* o "ICO", sarebbe quindi possibile riferire una transazione sulla *blockchain* ad un bene presente nella realtà materiale (come un segreto commerciale), attraverso la specificazione del bene stesso all'interno dei metadati associati alla transazione, frazionando e tokenizzando il diritto ai ricavi futuri dello sfruttamento di diritto di proprietà intellettuale. I token che rappresentano segreti commerciali sono infatti scambiabili, rappresentabili nella categoria degli asset token e *non-fungible* token (NFT), formando un mercato secondario estremamente liquido che, in virtù della programmabilità, potrebbe essere la base per lo sviluppo di altre applicazioni. La stessa *blockchain* è infatti considerata un "*internet of value"*, in quanto permette la circolazione di valore. Il pagamento dei token generalmente avviene con valute virtuali in luogo di moneta avente corso legale, senza alcun vincolo territoriale, né per quanto attiene alla figura dell'emittente né per quella del promotore. Con l'ICO può essere pubblicato in allegato un c.d. "*white-paper*" in luogo di un prospetto, nel quale vengono riportate le principali caratteristiche e condizioni dell'operazione e dell'oggetto dell'offerta. Le ICO, a livello di mercato primario, possono dunque essere utilizzate dai titolari di segreti commerciali come modalità di finanziamento delle loro attività imprenditoriali, mediante ricorso a forme di appello al pubblico risparmio[230].

È importante però fare un appunto per ciò che concerne il valore probatorio della certificazione del deposito. Il codice *hash,* che costituisce l'impronta digitale crittografica di un bene digitale iscritto nel registro, può venir utilizzato come prova della paternità di un'opera e inoltre, come già illustrato, la notarizzazione è utile per ottenere una rappresentazione certificata della data e dell'orario di deposito della registrazione. Tuttavia, a livello legislativo in Italia manca ancora una definizione chiara della portata probatoria di queste certificazioni. Infatti, sebbene la materia sia trattata all'interno dal quadro legislativo

---

[229] Si veda in tal senso G. FREZZA, *Blockchain, autenticazione e arte contemporanea,* in *Dir. fam*., 2020, II, 489, e M. MAUGERI, (nt. 226), 375, D. AQUARO, (nt. 221), 10 e V. MOSCON, (nt. 215), 140. Un esempio di *smart contract* è Etherisc, un'assicurazione sui viaggi aerei decentralizzata, che opera sulla piattaforma *blockchain* Ethereum. Lo *smart contract* interroga delle Api (interfacce per la programmazione di applicazioni,) per avere informazioni sugli orari di partenza e, in caso di ritardo del volo aereo garantito dalla polizza, fa scattare automaticamente il rimborso. La *blockchain* Ethereum è stata progettata propriamente per la scrittura di *smart contract*s, che consentono la definizione dei termini dello scambio e il trasferimento di valori anche diversi rispetto alla criptovaluta. Si veda in tal senso M. MAUGERI, (nt. 226), 380.

[230] Il funzionamento delle ICO è descritto da G. GITTI, M. MAUGERI, C. FERRARI, (nt. 228), 98 e F. BRUSCHI, (nt. 217), 164.

italiano sulla "catena dei blocchi", norma risalente a febbraio 2019, quando il decreto legge semplificazioni è stato convertito in legge, introducendo la definizione di *blockchain* come "tecnologie basate su registri distribuiti", l'Agenzia per l'Italia digitale non ha ancora definito gli standard tecnici e le linee guida richiesti alle tecnologie *blockchain* per produrre gli effetti giuridici della validazione temporale elettronica. Anche a livello giurisprudenziale manca una definizione chiara nel merito, non essendosi ancora verificata una "causa-pilota" in grado di spingere i giudici a pronunciarsi sull'efficacia della certificazione tramite *blockchain*[231].

Le evidenze informatiche delle transazioni registrate sulla *blockchain* rientrano però nell'ambito del Regolamento UE eIDAS 2014/910 (da ora eIDAS), come documento elettronico con "contenuto conservato in formato elettronico", nonché di quello di documento informatico contenuta nel Codice dell'Amministrazione digitale. Come disciplinato all'art. 46 del Regolamento eIDAS, alle evidenze informatiche non potranno essere negati gli effetti giuridici e dovranno comunque essere ammessi come prova nei procedimenti giudiziali. Tuttavia, se le transazioni vengono create attraverso l'utilizzo di chiavi crittografiche, ciò non soddisfa i requisiti previsti per le firme elettroniche avanzate, lo stesso eIDAS richiede che le transazioni debbano essere connesse univocamente al firmatario ed idonee a identificarlo, requisiti non presenti nelle reti *blockchain* di tipo pubblico o *permissionless*; oltre a ciò, la normativa italiana richiede ulteriori adempimenti, stabiliti dall'art. 55 ss. del D.P.C.M. del 22 febbraio 2013, come l'identificazione certa del firmatario, un sistema di revoca del consenso e la sottoscrizione di un accordo per l'utilizzo della firma elettronica, tutti elementi che non si conciliano con le tipologie di *blockchain* fin qui indicate. Tali considerazioni potrebbero perciò portare ad escludere la possibilità di fornire alle transazioni iscritte nella *blockchain permissionless* rilevanza e valenza probatoria, ma d'altra parte lo stesso art. 46 eIDAS e l'art. 20, co. 1-*bis,* del Codice dell'Amministrazione digitale prevedono che al documento elettronico vengano riconosciuti effetti giuridici, pertanto sarà il giudice a dover valutare

---

[231] Per questioni di carattere legislativo si veda l'articolo di D. AQUARO, (nt. 221). Si rileva a livello internazionale una sola decisione in materia, richiamata da F. SARZANA *Copyright: il valore della blockchain come strumento di prova nel processo civile,* IlSole24Ore, 2018, dove si legge che il Tribunale di Hangzhou, in Cina, il 28 giugno 2018, è diventato il primo organismo giudiziario al mondo ad aver acconsentito l'uso della tecnologia *blockchain* per l'archiviazione di prove da produrre in giudizio. Il Tribunale cinese si è pronunciato in una disputa sul diritto di divulgare opere al pubblico su reti di informazione, stabilendo che l'uso della tecnologia *blockchain* per l'archiviazione delle prove per via elettronica era un sistema legalmente ammissibile. La Corte del capoluogo della provincia cinese di Zhejiang ha affermato così che l'uso della suddetta tecnologia *blockchain* da parte dell'attore per archiviare le prove era uno strumento pienamente compatibile con il codice di procedura civile cinese, pronunciandosi a favore dell'attore, per una violazione addebitata al convenuto proprio accertata sulla base di questa prova.

l'idoneità stessa a soddisfare i requisiti di legge, determinandone l'efficacia probatoria, tenuto conto delle caratteristiche di sicurezza e integrità. Ma qui ci si ricollega alla questione prima posta, ossia al fatto che nella giurisprudenza italiana manca ancora una causa pilota o una trattazione approfondita della tematica[232].

Nonostante ciò, sempre più organizzazioni economiche stanno implementando sistemi per la tutela di segreti commerciali, marchi, brevetti e opere autoriali tramite la tecnologia *blockchain*. Questo strumento diverrà sempre più una soluzione aggiuntiva per le imprese, che avranno così ulteriori possibilità di archiviare le prove relative all'uso dei loro marchi e dei documenti relativi alle opere di qualsiasi tipo, mettendo in sicurezza il proprio know-how, digitalizzando gli allegati contrattuali relativi ai diritti di proprietà, mentre risulta ancora distante l'ipotesi di una piena sostituzione dei registri pubblici di brevetti, come i registri gestiti dall'EUIPO o dal WIPO.

Per concludere, focalizzandoci sui segreti commerciali, si può tranquillamente intendere la *blockchain* come uno strumento sicuro per il caricamento delle informazioni nel rispetto del requisito delle "misure ragionevoli", come richiesto dall'art. 98 c.p.i., data l'estrema difficoltà, se non addirittura impossibilità, di *hacking* della catena, e una possibile modalità di finanziamento delle attività imprenditoriali attraverso il processo di tokenizzazione dei segreti commerciali e di ICOs. Dato però il particolare momento di transizione della materia, si ritiene opportuno affidare solamente i segreti di minore importanza a questo sistema di protezione*,* attendendo che, anche nel nostro paese, ci sia una piena e concreta definizione della tecnologia sia a livello legislativo che giurisprudenziale[233].

4.5. Cenni su GDPR, normativa trattamento dei dati personali

Con lo sviluppo dell'intelligenza artificiale e dei sistemi di trattamento degli algoritmi sono nate numerose tecnologie capaci di impiegare i dati personali provenienti dal mondo online, da cui ricavare informazioni per scopi di natura prettamente commerciale. I dati sono diventati così beni di consumo e di scambio da cui estrapolare informazioni, fonte di vantaggi

---

232 Sulla valenza probatoria e rilevanza delle transazioni su *blockchain* si veda F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 58 SS.

233 Si veda anche A. BALBO, (nt. 214), che sottolinea l'elevato livello di sicurezza delle piattaforme *blockchain*; per accedere a tali reti, infatti, sarebbero necessarie le chiavi di accesso e, inoltre, nell'improbabile caso di *hacking*, l'hacker dovrebbe modificare i dati in ogni singolo nodo del sistema (si definisce "nodo" ogni computer e dispositivo connesso alla rete) lasciando, quindi, informazioni e tracce rilevanti che consentirebbero al detentore del segreto commerciale di risalire all'autore della violazione.

competitivi per le imprese, o di profitti economici per gli enti privati; le informazioni ricavate da questi strumenti possono infatti essere vendute a terzi che a loro volte le possono sfruttare per finalità diverse, come per scopi di marketing o per scopi meramente pubblicitari, oppure come supporto alla ricerca scientifica[234].

La tecnologia alla base di questo processo agisce attraverso un sistema di aggregazione, che, analizzando e identificando le possibili correlazioni tra la moltitudine di dati presenti in rete, riesce a creare dei modelli che diventano dei veri e propri elementi di supporto del management nella determinazione delle scelte strategiche delle imprese. Tutte le informazioni ottenute da tali processi vanno a costituire quello che è l'asset immateriale dell'impresa, asset che gode di una valenza strategica-competitiva notevole per le attività imprenditoriali, si pensi agli elenchi di clienti e relativi dati, analisi di mercato, informazioni su acquisti, costi o prezzi[235]. Si è già evidenziato in questo elaborato come sia la tecnologia di elaborazione di tali dati, sia risultati da essi ottenuti, possono essere oggetto di tutela come diritti di proprietà intellettuale, in particolar modo tramite la tutela come segreti commerciali. Questi asset immateriali sono infatti diventati capitali sempre più considerevoli del patrimonio delle imprese, essendo nuove tecnologie e processi capaci di far acquisire vantaggi competitivi rispetto i *competitors*.

Tuttavia, parallelamente al crescere di questi nuovi sistemi, è stato necessario prevedere delle discipline per la protezione e il trattamento dei dati personali. Proprio in quest'ottica l'Unione europea ha emanato il regolamento 679/2016 (d'ora in poi definito come GDPR), regolamento entrato in vigore il 24 maggio 2016 ma con operatività in Italia a partire solamente dal 25 maggio 2018, contemporaneamente all'entrata in vigore del regolamento

---

234 In tal senso si è espresso I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali,* in *ODCC*, 2018, 69 ss., sottolineando come lo sfruttamento commerciale delle informazioni personali, qualificabili come beni immateriali disponibili e vendibili, rappresenta una delle principale attività delle imprese che forniscono servizi di tipo digitale e un elemento assolutamente dominante nelle economie digitali moderne. Per dato personale s'intende qualsiasi informazione riguardante una persona fisica identificata o "identificabile", ossia una persona fisica che può essere identificata con un particolare riferimento come può essere il nome, un numero di identificazione, dei dati relativi all'ubicazione, un identificativo online o caratteristiche dell'identità fisica, genetica, psichica, economica, culturale o sociale, si veda in tal senso C. NOCERA, in *Il nuovo regolamento privacy,* Maggioli Editore, Rimini, 2018, 9.

235 Tutti gli elementi qui elencati sono presentati nel rapporto dell'European IPR Helpdesk, (nt. 166), 2, tra le tipologie di informazioni tutelabili come segreto commerciale. Come indicato nel rapporto, queste informazioni possono essere utilizzate come strumento per la competitività delle imprese e per la gestione dell'innovazione nella ricerca, aiutando a raggiungere la competitività sul mercato attraverso la promozione dell'innovazione, spesso fulcro delle operazioni di un'impresa.

privacy n. 2016/679[236]. È dunque importante sottolineare che il regolamento GDPR presenta una forte connessione con la direttiva UE 2016/943 (si veda *supra* 1.2.) in materia di tutela di segreti commerciali, in quanto entrambe le discipline sono venute a costituirsi come una pronta risposta regolatoria al fenomeno "dell'algoritmizzazione" del settore digitale[237].

Il regolamento GDPR non viene dunque a costituirsi solo in una logica di tutela dei dati personali, riconosciuto già come diritto fondamentale dalla UE all'art. 8 della Carta dei diritti dell'UE, in ottemperanza della non meno importante garanzia di libera circolazione dei dati personali nel territorio degli Stati membri, ma di fatto il GDPR rappresenta la base della visione europea per lo sviluppo dell'economia digitale ed è per questo motivo che è necessaria la sua trattazione in questo elaborato. Il GDPR può essere così definito come un "baricentro", capace di bilanciare da una parte i diritti e le libertà fondamentali dei cittadini europei, e dall'altra, di favorire la libera circolazione dei dati all'interno dell'Unione, permettendo alle imprese di sfruttare tutte le rilevanti possibilità connesse a questo settore, sostenendo la costituzione di una società digitale a misura della persona umana[238].

Il principio di trasparenza risulta il cardine della disciplina GDPR, definendo l'intero ciclo di trattamento dei dati, dalla progettazione delle tecnologie responsabili delle elaborazioni fino al momento del controllo successivo delle conseguenze scaturenti dalle stesse operazioni di trattamento dei dati. Il principio di trasparenza del GDPR è riconnesso a tre principali categorie di disposizioni che vengono illustrate nel regolamento: *in primis* al diritto alla spiegazione, cioè al diritto, del singolo soggetto interessato, di ottenere da parte dell'impresa titolare del trattamento tutte le informazioni "significative" sulla logica e finalità del trattamento automatizzato impiegato, limitatamente però ai soli *input* e *output* del processo

---

236 GDPR è un acronimo in inglese di *General Data Protection Regulation,* in italiano Regolamento Generale sulla Protezione dei Dati, in sigla anche RGPD. Con l'entrata in vigore del decreto legislativo del 25 maggio 2018, il Codice in materia di protezione dei dati personali di cui al decreto legislativo 20 giugno 2003, n. 196 verrà integrato con le nuove previsioni regolamentari previste dal GDPR, in tal senso si veda C. NOCERA, (nt. 234), 10. Per trattamento di dati personali s'intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insieme dei dati, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adeguamento, modifica, trasmissione e comunicazione, cancellazione e distruzione.

237 In tal senso si è espressa G. SCHNEIDER, *Verificabilità del trattamento automatizzato dei dati personali e tutela del segreto commerciale nel quadro europeo,* in *Merc., conc., reg.*, 2019, II 354.

238 Così sono espressi anche G. D'ACQUISTO, F. PIZZETTI, in *Regolamentazione dell'economia dei dati e protezione dei dati personali,* in *AGE*, 2019, I, 89 ss. Questo è evidente dai Considerando 5 e 6 del GDPR, in cui ripetutamente si sottolinea lo stretto legame tra la libera circolazione dei dati nella UE e lo sviluppo delle nuove tecnologie e dell'economia digitale, fino ad affermare, in particolare nel Considerando 5, che: "Il diritto dell'Unione impone alle Autorità degli Stati membri di cooperare e scambiarsi da personali per essere in grado di svolgere le rispettive funzioni".

algoritmico che l'utente è in grado di comprendere, in tal modo il GDPR garantisce il rispetto di tutti gli altri diritti presenti nel regolamento, come ad esempio, il diritto all'oblio o alla portabilità dei dati[239].

La seconda disposizione che costituisce il principio di trasparenza è connessa dal potere di revisione dei trattamenti automatici che sono posti in capo alle autorità di controllo: il GDPR assegna poteri di indagine alle autorità di controllo, in modo tale da verificare la correttezza della progettazione e l'evoluzione strutturale degli algoritmi processanti dalle imprese, al fine di monitorare la liceità e la correttezza dei trattamenti medesimi e di rilevare, dunque, eventuali schemi algoritmici discriminatori[240].

Da ultimo, il principio di trasparenza è completato dall'obbligo della valutazione sull'impatto dei trattamenti sviluppati, riferiti principalmente all'identificazione di quelle proprietà strutturali e funzionali dei metodi di trattamento algoritmici. Questo può essere eseguito tramite un *auditing* interno o esterno, affidato quindi a tecnici dipendenti o imprese terze esperte, ciò servirà a determinare le c.d. "valutazioni d'impatto" tramite delle vere e proprie investigazioni tecniche applicate ai meccanismi di funzionamento delle architetture computazionali. Le imprese dovranno pertanto predisporre procedure e misure in grado di prevenire errori, imprecisioni e fattori discriminanti nel corso del trattamento dei dati personali[241].

---

[239] Come indicato dagli art. 13-15 GDPR. Il titolare del trattamento è tenuto all'adozione di misure appropriate, in moto tale da fornire al soggetto interessato tutte le informazioni relative al trattamento in forma semplice e accessibile, utilizzando un linguaggio chiaro. Si veda anche in tal senso C. NOCERA, (nt. 234), 21. Il GDPR prospetta una certa libertà di forma, le informazioni possono essere fornite per iscritto o con altri mezzi, anche elettronici, se richiesto dall'interessato, la direttiva prevede che le informazioni possano addirittura essere fornite oralmente. Per ciò che concerne il diritto all'oblio, s'intende il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, mentre per portabilità dei dati s'intende il diritto dell'interessato di ricevere un format strutturato con i dati personali che lo interessano.

[240] Come indicato dall'art. 58 GDPR. Rileva C. NOCERA, (nt. 234), 43, che il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il relativo rappresentante, devono fornire, su richiesta, piena cooperazione con l'autorità di controllo nell'esecuzione dei loro compiti d'indagine.

[241] Come indicato dall'art. 29 definito come il "*Working Party*" e dall'art. 35 GDPR. In tal senso si veda G. SCHNEIDER, (nt. 230), 364, che, nel definire i controlli sui sistemi di protezione dei dati, chiarisce la differenza tra le indagini eseguite dalle autorità di controllo statale e gli *auditing* interni o esterni compiuti nella valutazione d'impatto: il potere di condurre indagini sotto forma di attività di revisione sulla protezione dei dati è assegnato, come indicato dall'art. 58, co. 1, lett. a) GDPR alle autorità di controllo nazionali. Dalla stessa normativa si disciplina che, ai fini della revisione algoritmica, le stesse autorità di controllo hanno anche il potere di "ottenere dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie" per l'esecuzione del loro compito investigativo. A questo potere di indagine delle autorità corrisponde il dovere delle imprese titolari del trattamento di condurre le c.d. "valutazioni d'impatto sulla protezione dei dati e di consultazione preventiva", come previsto dall'art. 35 GDPR. Si tratta di un documento che determina tutti i rischi inerenti "i diritti e le libertà delle persone fisiche", o un trattamento che prevede "l'uso di nuove tecnologie".

Il GDPR, e il principio di trasparenza ad esso connesso, sono volti a prevenire o limitare possibili eventi pregiudizievoli conseguenti al trattamento illecito dei dati personali da parte dei proprietari del trattamento stesso. In questo contesto, prima dell'introduzione del GDPR, il rapporto presentava infatti una forte asimmetria, dato che il soggetto interessato al trattamento dei dati personali risultava in una posizione di maggiore debolezza; è stato quindi necessario aumentare la protezione per questi soggetti "deboli". Proprio con questo obiettivo viene a realizzarsi la disciplina del GDPR, che agendo tramite il principio di trasparenza e il principio di responsabilità ad esso ricollegato, è intervenuta limitando fortemente tale asimmetria[242].

Dati gli aspetti fin qui illustrati, la disciplina del GDPR sembra porsi in contrapposizione con quelli che sono invece gli ambiti applicativi della tutela delle informazioni come segreto commerciale. In particolare, ci si può porre la questione di come tutelare le informazioni che alimentano (in *input*) e vengono create (in *output*) dai sistemi di trattamento automatizzato e al contempo rispettare correttamente quelle che sono le prescrizioni dettate dal GDPR: il rilascio di informazioni, sia in *input* che in *output,* inerenti il trattamento potrebbero arrecare alle imprese utilizzanti le tecnologie algoritmiche forti pregiudizi, dato che le imprese concorrenti potrebbero più facilmente acquisire il loro know-how tecnico, o addirittura pregiudicare una possibile tutela come segreto commerciale di tali informazioni. Il principio stesso di trasparenza può sembrare antitetico rispetto al mantenimento in segretezza delle informazioni, delineando così un conflitto tra le esigenze di protezione della proprietà intellettuale e la protezione dei dati personali stabiliti dal GDPR[243].

Si ritiene che una corretta risoluzione di questa problematica possa essere trovata operando un

---

242 La presenza di un rapporto asimmetrico è stato evidenziato da numerosi autori, si veda in tal senso E. TOSI, in *La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR),* in *Studium Iuris*, 2020, IX, 1032 ss., in cui, trattando ulteriormente la trattazione del principio di responsabilità, si ritiene accolta positivamente la qualificazione della speciale responsabilità civile per trattamento illecito di dati personali, come disciplinato dall'art. 82 GDPR. In termini di responsabilità oggettiva per rischio d'impresa, derivante dall'attività di trattamento dei dati personali in violazione delle regole di condotta confermative e protettive dell'interessato-danneggiato, il soggetto risulterebbe debole in un rapporto asimmetrico, e questo sarebbe dovuto allo stesso trattamento dei dati personali. La presenza di un'asimmetria informativa nel rapporto tra le parti è rilevata anche da G. SCHNEIDER, (nt. 237), 378, indicando come la *ratio* ultima del diritto in materia è quella di mitigare le asimmetrie informative presenti tra le imprese processanti i dati e i soggetti interessati, tutelando il diritto degli stessi a autodeterminarsi nelle dinamiche dei mercati digitali.

243 Si veda in tal senso G. SCHNEIDER (nt. 237), 372, in cui s'indica che la tutela dell'informazione come segreto commerciale ha diretti riflessi sul piano *intra*-sistemico e *extra*-sistemico, relativamente all'interazione dello stesso sistema dei diritti di proprietà intellettuale con altre normative, come nel caso della normativa GDPR. In particolare, è proprio sul piano *extra*-sistemico che ci si focalizza in questo paragrafo, valutando l'interazione "orizzontale" della tutela del segreto con altri diritti di senso contrario e postulanti la trasparenza delle informazioni relative alle tecnologie processanti.

certo bilanciamento tra le due discipline: il GDPR dovrà venir applicato seguendo una logica di tipo proporzionale, valutando l'ambito specifico del caso e non pregiudicando nella sua attuazione i diritti di proprietà intellettuale, garantendo, parallelamente, il rispetto di quelle che sono le disposizioni previste dal GDPR; si provvederà così ad un bilanciamento che permetterà sia il rispetto dei diritti di proprietà intellettuale che un corretto trattamento dei dati personali[244]. La stessa direttiva UE 2016/943 precisa la necessità di un bilanciamento, tant'è che all'art. 34 afferma che: "*La direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta, nella fattispecie* […] *il diritto alla protezione dei dati personali*", nell'art. 35 della direttiva si aggiunge inoltre che: "*È importante che siano rispettati i diritti al rispetto della vita privata e familiare, nonché alla protezione dei dati personali di tutti coloro i cui dati personali possono essere oggetti di trattamento*"[245].

Dunque, l'impresa dovrà prevedere un regime di tutela "modulata" del segreto relativo al

---

[244] In tal senso si sono espressi E. TOSI, (nt. 242), 1038 e G. SCHNEIDER (nt. 237), 364, per i quali è necessario far riferimento al considerando n. 63 GDPR in cui è precisato che: "Ove possibile il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software". Al riguardo, si veda anche il considerando n. 4 GDPR, in cui si precisare che: "Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità", tra questi diritti fondamentali si rinviene certamente al diritto della libertà d'impresa.

[245] Si veda G. SCHNEIDER, (nt. 237), 376, in cui si indica come il principio di proporzionalità ha una forte importanza in quanto risulta un parametro fondamentale nell'operazione di bilanciamento tra diritti di proprietà intellettuale e il diritto al rispetto della vita privata. Tale principio è stata riaffermato da una pronuncia della stessa Corte di Giustizia, la quale ha precisato come le limitazioni ai diritti e alle libertà riconosciuti dalla Carta di Nizza debbano rispettare "il contenuto essenziale di detti diritti e libertà". Il sistema di bilanciamento tra l'applicazione delle disposizioni del GDPR e la tutela dei diritti di proprietà industriale è stato recentemente confermato dalla giurisprudenza italiana dal T.A.R. del Lazio, relativamente alla richiesta di accesso alle informazioni funzionali di una procedura automatizzata utilizzata dal Ministero dell'Istruzione per il trasferimento interprovinciale dei docenti. Il T.A.R. Roma, (Lazio), sez. III, 21 marzo 2017, n. 3742, in *DeJure* ha precisato che: "La disciplina dettata a tutela del diritto di autore e della proprietà intellettuale è funzionale a garantire gli interessi economici dell'autore, ovvero del titolare dell'opera intellettuale, mentre la normativa sull'accesso agli atti è funzionale a garantire altri interessi e, in questi limiti, deve essere consentita la visione e anche l'estrazione di copia; né il diritto di autore né la proprietà intellettuale precludono la semplice riproduzione, ma precludono, invece, al massimo, soltanto la riproduzione che consenta uno sfruttamento economico e, non essendo l'accesso lesivo di tale diritto all'uso economico esclusivo dell'opera, l'ostensione deve essere consentita nelle forme richieste da parte dell'interessato, ossia della visione e dell'estrazione di copia, fermo restando che delle informazioni ottenute dovrà essere fatto un uso appropriato, ossia esclusivamente un uso funzionale all'interesse fatto valere con l'istanza di accesso che, per espressa allegazione della parte ricorrente, è rappresentato dalla tutela dei diritti dei propri affiliati, in quanto ciò costituisce non solo la funzione per cui è consentito l'accesso stesso, ma nello stesso tempo anche il limite di utilizzo dei dati appresi, con conseguente responsabilità diretta dell'avente diritto all'accesso nei confronti del titolare del software. […] Tenere ben distinte le due fattispecie è essenziale per calibrare i diversi interessi in gioco allorché si renda necessario un bilanciamento caso per caso tra tali interessi". G. SCHNEIDER, (nt. 237), 375, commentando tale sentenza, sostiene che, il T.A.R. del Lazio ha proposto un approccio sistematico alla delimitazione dei diritti di proprietà intellettuale, rispetto a quello che può essere l'ambito di applicazione di altre normative, non oltre quanto sia proporzionalmente necessario e così da garantire una piena protezione di quelli che sono gli interessi sottesi alla relativa disciplina.

trattamento automatizzato di dati personali, così da poter garantire i propri diritti, rispettando parimenti la disciplina prevista dal GDPR. Se analizziamo infatti più approfonditamente le tre disposizioni che costituiscono il principio di trasparenza, elemento che abbiamo definito come centrale nel regolamento GDPR, si può notare come il diritto alla spiegazione non preclude di per sé la tutela alla segretezza, in quanto le informazioni hanno come possibili destinatari singoli soggetti interessati e non imprese concorrenti. Il potere di revisione sui metodi di applicazione del trattamento dei dati affidato alle pubbliche autorità non può venir limitato dalla presenza di segreti commerciali, in quanto, come disposto dalla direttiva UE 2016/943, la presenza di un segreto commerciale non limita le disposizioni relative alle attività di revisione delle autorità di controllo, quindi l'acquisizione di informazioni da parte di queste autorità sono pienamente lecite, fatti comunque salvi gli obblighi di riservatezza a cui questi soggetti sono tenuti[246]. Infine, alcune problematiche potrebbero venir evidenziate nel sistema di salvaguardia del segreto commerciale in caso di *auditing,* che ricordiamo essere attività effettuata per le necessarie valutazioni sull'impatto dei trattamenti sviluppati. In particolare, il problema si pone per gli *auditing* di tipo esterno che sono affidati a imprese terze: pur non risultando pregiudizi particolari di natura concorrenziale, in ogni caso, per limitare quanto più possibile i rischi connessi a queste attività di *auditing*, possono venir sviluppati strumenti esoaziendali di tutela delle informazioni segrete, quale la stipula di NDA con tali imprese terze (si veda *supra* 3.3.1.)

Si può quindi concludere affermando che la tutela modulata del segreto permette il trattamento automatizzato dei dati personali nel rispetto della normativa GDPR: i soggetti interessati saranno così informati riguardo il trattamento di detti dati, le autorità di controllo eserciteranno i propri poteri di revisione e le società terze di controllo potranno condurre le valutazioni d'impatto necessarie. Le discipline si completano così a vicenda, costituendo un sistema rispettoso dei diritti fondamentali dell'uomo e permettendo, al contempo, possibili ulteriori crescite del settore e delle opportunità connesse al trattamento dei dati personali.

---

[246] Si veda in tal senso l'art. 11 della direttiva UE 2016/943, dove si prevede che: "La direttiva non dovrebbe pregiudicare l'applicazione delle norme dell'Unione o nazionali che prevedono la divulgazione di informazioni, inclusi i segreti commerciali, al pubblico o alle autorità pubbliche, né essa dovrebbe pregiudicare l'applicazione delle norme che consentono alle autorità pubbliche di raccogliere informazioni per lo svolgimento dei loro compiti". Si veda anche l'art. 18, in cui s'indica che il controllo sul trattamento del dati: "Non dovrebbe pregiudicare eventuali obblighi di riservatezza per quanto concerne il segreto commerciale o eventuali limitazioni al suo utilizzo, che il diritto dell'Unione o nazionale impongono al destinatario delle informazioni o al soggetto che le acquisisce. In particolare, la direttiva non dovrebbe esonerare le autorità pubbliche dagli obblighi di riservatezza cui sono soggette in relazione alle informazioni trasmesse dai detentori di segreti commerciali, a prescindere dal fatto che tali obblighi siano sanciti dal diritto dell'Unione o da quello nazionale".

4.6. La normativa *cybersecurity*

La direttiva UE 2016/943 ha ridefinito la normativa in materia di segreti commerciali (si veda *supra* 1.2.) ponendo particolare attenzione sull'adozione di adeguate misure di sicurezza per la tutela delle informazioni riservate. Tale normativa, tuttavia, non indica quali siano esattamente le azioni e le misure da adottare, un aiuto in tal senso può provenire dalla prassi e dalla definizione delle fasi di costituzione del segreto commerciale, ma anche da normative dettate per temi differenti, che risultano in qualche modo assimilabili, come nel caso del regolamento GDPR e della direttiva UE NIS 2016/1148, entrata in vigore il 6 luglio 2016, che da ora definiremo come la "normativa *cybersecurity*", ossia la direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea[247].

La normativa *cybersecurity* nasce con l'obiettivo di disciplinare lo spazio cibernetico inteso come il *network* delle infrastrutture della *information tecnology,* inclusivo delle rete internet, del sistema di telecomunicazioni e dei sistemi informatici, costituito da infrastrutture interconnesse. Lo spazio cibernetico è composto da dispostivi sia hardware che software, ed è uno spazio all'interno cui vengono trasferiti e connessi dati ed utenti generando delle relazioni logiche tra sistemi. Data l'estensione globale delle comunicazioni, lo spazio cibernetico presenta elevati rischi, rischi che possono causare danni di natura patrimoniale alle imprese, ma anche possibili conseguenze pregiudizievoli alle cose o alle persone[248].

Nello spazio cibernetico sono i dati la principale risorsa e, giacché il loro valore commerciale è in costante crescita, il legislatore ha disciplinato la necessità per le organizzazioni proprietarie di tutelarne il valore garantendo che lo spazio cibernetico, in cui i dati vengono trasferiti e comunicati, sia un ambiente sicuro e protetto. Ciò può essere garantito attraverso l'adozione di idonee misure di protezione a livello sia fisico che logico e procedurale, assicurando così la solidità delle reti e dei dispositivi informatici rispetto a possibili eventi di natura volontaria o casuale che potrebbero determinare l'acquisizione e il trasferimento indebito di dati, o la loro modifica o distruzione illegittima, ovvero il controllo indebito, attraverso il danneggiamento, la distruzione o il blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi. In queste disposizioni vediamo una congruenza con le normative, sia europea che italiana, in materia di tutela di segreti

---

[247] La direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi è stata recepita dall'ordinamento italiano attraverso il d.lgs. 18 maggio 2018, n.65 in vigore dal 24 giugno 2018.

[248] Come indicato da S. LANDINI, in *Cyber risk: le polizze assicurative per tutelarsi,* in *Quot. Giur.*, 2018, 1.

commerciali: sia nella normativa *cybersecurity* che nelle disposizioni di legge inerenti l'istituto del segreto il fine ultimo è quello di tutelare l'informazione, sia esso un dato o know-how di natura tecnico-commerciale; le imprese per tutelare le proprie informazioni digitali, come segreti commerciali, possono dunque correttamente seguire le disposizioni della normativa *cybersecurity* per garantire l'adeguatezza delle misure di protezione e valorizzarne così il know-how in esso contenuto. Il tema della *cybersecurity* è dunque di centrale importanza per tutte quelle realtà imprenditoriali che operano nel settore digitale o che sfruttano gli strumenti digitali, non solo nell'ottica del rispetto delle relative norme, ma anche come investimento nella tutela dei propri diritti di proprietà intellettuale[249].

Secondo le disposizioni dell'Unione Europea, per *cybersecurity* s'intendono infatti tutte le "*misure di salvaguardia e le azioni che possono essere utilizzate per proteggere lo spazio cibernetico, da quelle minacce che sono associate o che possono danneggiare le sue reti interdipendenti e la sua infrastruttura informativa. Con la sicurezza informatica ci si impegna a preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni in esse contenute*" mentre, nelle fonti italiane, la *cybersecurity* viene definita come la "*pratica che consente a un'entità (ad esempio, un'organizzazione, un cittadino, o una nazionale ecc.) la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyberspace"*. Principi base della sicurezza *cyber* sono dunque la disponibilità, l'integrità e la confidenzialità, non solo di dati e informazioni, ma anche dei sistemi e delle reti che la compongono, in modo tale da ritenere l'intero spazio cibernetico sicuro[250].

Nella normativa *cybersecurity* si stabilisce che gli operatori di servizi essenziali e i fornitori di servizi digitali devono adottare un processo di adeguamento costituito da *steps* di *assessment*, *remediation* e monitoraggio al fine di individuare le misure tecniche e organizzative adeguate a proteggere sistemi e reti informatiche, ossia le stesse fasi che abbiamo già incontrato nel capitolo 2 valutando il possibile processo per la costituzione di un segreto commerciale; ciò conferma come la normativa *cybersecurity* sia un'utile parametro di riferimento per tutte quelle imprese che vogliono costituire un sistema di protezione adeguato al mantenimento

---

[249] In tal senso si veda S. LANDINI, (nt. 248), 1. La definizione di spazio cibernetico è riscontrabile in Italia nel decreto recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali nel D.P.C.M., 17/02/2017 , G.U. 13/04/2017.

[250] Come esposto da B. PANATTONI, (nt. 170), 5.

della segretezza delle proprie informazioni[251].

Con la direttiva NIS l'Unione europea ha creato un'evoluzione "trasformativa" della sicurezza informatica, attraverso maggiori iterazioni tra pubblico e privato, la collaborazione tra Stati membri, la definizione di standard e procedure comuni, individuando autori competenti a gestire eventuali crisi, prevedendo obblighi, responsabilità e sanzioni, creando così un sistema strutturato per la protezione sia degli operatori di servizi essenziali, sia dei dati e informazioni di utenti, imprese e cittadini. L'effetto della normativa *cybersecurity* ha così una portata globale, agendo in profondo, rafforzando complessivamente la sicurezza europea tramite un'insieme di misure per la protezione dei dati della comunicazione, della logistica, nella tutela delle risorse, dei diritti di proprietà intellettuale e dei vantaggi economici connessi[252].

In sintesi, si può dunque sostenere che le adeguate misure rinvenibili nella normativa in tema di *cybersecurity* sono utili sia per la costituzione di un processo che garantisca la protezione delle reti e dei sistemi informatici, ma anche per la protezione di know-how e segreti commerciali. E non potrebbe essere altrimenti: la stessa protezione delle informazioni segrete necessita che la rete e i sistemi informatici in cui questi sono contenuti risulti sicura, in particolar modo oggi, dato che dalle ultime analisi si riscontra che il 23% delle imprese in Italia ha subito almeno sette *cyber*-attacchi nell'ultimo anno[253].

4.7. Cenni su *big data*

La rivoluzione digitale in atto ha reso sempre più importante il ruolo svolto nel mercato dalle imprese che operano nel settore della *digital economy,* imprese che sfruttano le tecnologie connesse alla *big data analytics* operando attività di "*data-driven innovation*". Queste attività

---

[251] Nel rapporto NIS vengono definiti operatori di servizi essenziali tutte le imprese operanti nei settori dell'energia, dei trasporti, nel settore bancario e finanziario, nel settore sanitario, della distribuzione e fornitura di acqua potabile e delle infrastrutture digitali; mentre per servizi digitali si definiscono le imprese operanti nel mercato online, i motori di ricerca online, i servizi di *cloud computing*.

[252] In tal senso si veda l'articolo di G. TERZI, *Una nuova stagione per la cybersicurezza*, Ilsole24Ore, 2017, 10.

[253] Secondo le statistiche del *Cyber risk index,* reperibile in internet al seguente sito: https://www.trendmicro.com/it_it/about/newsroom/press-releases/2020/2021-01-12-cybersecurity-i-italia-e-in-zona-arancione.html#:~:text=Il%20Cyber%20Risk%20Index%20globale,indicando%20un%20%E2%80%9Crischio%20elevato%E2%80%9D. Si veda L. MAGNA, *Lupin 4.0, giù le mani dal segreto industriale!*, Industria Italiana, 2019, reperibile in internet al seguente sito: https://www.industriaitaliana.it/lupin-4-0-giu-le-mani-dal-segreto-industriale/, in cui si evidenza che, tra gli aspetti per una corretta gestione della sicurezza del know-how dell'impresa, è necessario prevedere una disponibilità dei dati, ossia salvaguardare il patrimonio informativo. La disponibilità dei dati dipende da diversi fattori che interferiscono tra utente e sistema, come: robustezza del software di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati e dal funzionamento o meno del sistema informatico, dal quale dipende anche la sicurezza dei dati in esso contenuti.

sono basate su processi di raccolta, immagazzinamento e analisi di grandi quantitativi di dati tramite l'uso di algoritmi sempre più sofisticati. Nell'attuale contesto digitale, considerato di *data-driven economy* (o economia dei dati), l'appartenenza di dati e informazioni assume un rilievo sempre più significativo, non solo per le imprese che implementano questo approccio decisionale sulla base delle informazioni oggettive ottenute dalla gestione dei *big data*, ma anche per gli stessi consumatori, che da queste tecnologie possono beneficiare di forti utilità, dato che le *data-driven companies* riescono ad offrire ai propri clienti servizi e prodotti ad un livello qualitativo migliore, con opzioni di vendita personalizzate, a prezzi più bassi rispetto quelli rinvenibili su mercati tradizionali[254].

Un'interpretazione simile è confermata dalla direttiva UE 2016/943 (si veda *supra* 1.2.), che definisce nel considerando 1 le informazioni create da processi di *big data*, *IoT* e intelligenza artificiale a "*moneta di scambio dell'economia della conoscenza*". Sono proprio i clienti delle imprese che concedono infatti l'uso dei propri dati per scopi di marketing, come per *mailing list,* in cambio dell'accesso ai vari servizi offerti dalle stesse imprese[255].

La strategia della Commissione Europea per il mercato unico digitale prevede proprio una promozione della *data-driven economy,* giacché nei mercati digitali sta oramai diventando imprescindibile la disposizione di dati e meta-dati degli utenti del web, come di dati di consumatori e clienti, tramite processi di raccolte e analisi, processi che possono venir effettuati direttamente dalle imprese oppure da società terze esperte in queste tipologie di servizi. Lo stesso termine *big data* viene giustificato dall'ubiquità e l'incommensurabilità di tale fenomeno, con caratteri di volume, varietà, velocità e veracità che attribuiscono, al suo detentore, un immenso valore economico in termini di potere di mercato[256].

---

[254] Come indicato da F. VESSIA, in *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, Milano, Giuffrè, 2019, 821. L'espressione "*Data-driven Innovation"* è stata usata come titolo del Report OECD, *Data-driven Innovation for Growth and Well-being*, 2014. Per *data-driven company* s'intende un'impresa che basa i suoi processi decisionali sui dati raccolti e sulle attività di elaborazione dei *big data.*

[255] In tal senso si sono espressi F. BANTERLE, M. BLEI, in *Alcune novità introdotte dalla direttiva Trade Secrets*, in *Dir. ind*., 2017, IV-V, 202.

[256] In letteratura si ritrovano molti riferimenti agli elementi identificativi delle quattro (o cinque V) che caratterizzano i *big data:* cfr. F. DI PORTO, *Big data e concorrenza*, in Conc. merc., 2016, XXIII, 6 ss. L'informazione, seconda l'autrice, ha sempre costituito il motore dell'economia, ma particolarmente nell'ultimo decennio il valore dell'informazione è cresciuto esponenzialmente, con un enorme impatto nel sistema economico e sociale. F. VESSIA, (nt. 254), 824, rileva che i *big data* possono assolvere a una diversa funzione rispetto l'oggetto dell'attività economica svolta. Per talune imprese, infatti, i dati raccolti costituiscono una semplice attività di input di informazioni, ossia un fattore che concorre alla creazione e implementazione dei business. Per altre, invece, i dati sono il risultato stesso dell'attività economica, e quindi il loro output. Queste ultime tipologie di imprese hanno dunque per oggetto la raccolta e la rivendita di dati attraverso processi di analisi di algoritmi e metadati.

Occorre però fare una distinzione tra dati personali e dati di tipo non personale: per dati personali s'intendono tutte le informazioni relative a una persona vivente identificata o identificabile, oppure tutte le varie informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona. Questi dati personali possono anche essere sottoposti a processi di deidentificazione, cifratura o pseudonimizzazione, ma se possono essere utilizzati per reidentificare una persona rimangono comunque dati personali, rientrando sempre nell'ambito di applicazione della normativa GDPR (si veda *supra* 4.5.). I dati personali spesso vengono divulgati alle imprese dagli stessi consumatori attraverso le piattaforme digitali, in cambio di servizi, o attraverso i social network, tramite la condivisione degli utenti dei social di informazioni, messaggi, foto e video. I dati personali possono venir divulgati alle imprese anche attraverso la navigazione online, tramite i cookies di ricerca, i quali catturano e memorizzano i siti visitati, la geolocalizzazione, o altre informazioni sulle abitudini dei consumatori, come le loro preferenze e i loro bisogni[257]. I dati non personali sono invece afferenti a fenomeni industriali, tecnici o naturali, oppure sono dati personali anonimizzati, in modo tale che l'individuo non sia o non sia più identificabile; perché i dati siano veramente anonimi il processo di anonimizzazione dovrà comunque essere irreversibile[258].

Nell'ordinamento giuridico italiano manca un'apposita disciplina di tutela della proprietà dei *big data*, sebbene la Commissione Europea stia valutando l'opportunità di creare un diritto di proprietà di tali dati, ci si pone ancora il quesito su come assicurare un certo livello di protezione giuridica a questo patrimonio immateriale. È necessario precisare che, mentre per i software e per l'hardware impiegato nell'elaborazione dei *data set* esistano strumenti di proprietà intellettuale, come il diritto d'autore e il brevetto, non sono invece presenti sistemi di tutela particolari per i dati in sé, sia con riferimento al *data set* alla base del procedimento di elaborazione, che per i risultanti di tali processi.

---

[257] La definizione di dato personale è rinvenibile nel sito della Commissione Europea, *Che cosa sono i dati personali,* reperibile in internet al seguente indirizzo: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_it. Sono esempi di dati personale: i nomi e cognomi, gli indirizzo di casa, gli indirizzi e-mail, il numero della carta d'identità, i dati sulla posizione o un indirizzo IP. Molti autori hanno analizzato le possibili tipologie contrattuali impiegabili per la trasmissibilità dei dati personali. Si evidenzia, in particolare, come la finzione della "gratuità" di molti servizi online, come nei social network, sono pagati col "prezzo" dei propri dati personali, si veda F. DI PORTO, (nt. 256), 13, in cui si aggiunge che questo sistema renderebbe applicabile la disciplina dei c.d. contratti del consumatore, con la conseguente nullità di molte delle clausole previste nei *terms and conditions* delle "app" e nei "social" più diffusi e conosciuti.

[258] Possono essere dati non personali: il numero di iscrizione al registro delle imprese di una società; indirizzo e-mail o tutti i dati resi anonimi.

La distinzione tra dati personali e non personali ha una forte implicazione sui possibili diritti di proprietà ad essi connessi, in quanto, nel primo caso, non è certo si possa configurare un vero e proprio diritto di proprietà su tali dati. Come disciplinato dal d.lgs. 196/2003 e successive modifcazioni e dal GDPR infatti si riconosce inderogabilmente la titolarità di questi dati alla persona a cui tali dati sono riferibili (il c.d. interessato), limitandone o condizionandone la libera trasferibilità. Tuttavia, la legge ammette che, una terza impresa, o un ente preposto possa, a certe condizioni, essere titolare del trattamento dei dati personali, il che può consentire a tale soggetto di conseguire anche il potere di sfruttarli economicamente. In particolare ciò avviene nell'ambito commerciale, dove il trattamento può consistere nel marketing diretto, come nella "profilazione", nella cessione o comunicazione a terzi per fini prettamente commerciali o pubblicitari[259].

Differentemente, per i dati di tipo non personale, sono possibili forme di appropriazione vera e propria, attraverso diritti di proprietà intellettuale sulle banche dati e, più precisamente, il diritto sui *generis*, o attraverso la disciplina del segreto commerciale. Queste tecniche sono comunque utilizzabili anche per i *data set* composti da dati di tipo personale per rafforzare il controllo che ne deriva dalla titolarità del trattamento[260].

Nonostante la disciplina del segreto commerciale non sia stata concepita prettamente per i *big data,* allo stato attuale risulta tra i migliori (e pochi) strumenti in grado di assicurare un certo livello di protezione giuridica a questa nuovo fondamentale strumento delle imprese. Perché si possa applicare la tutela come segreto devono però sussistere tutte le condizioni espresse dalla legge, ed è su questo delicato aspetto che concentreremo l'analisi in questo paragrafo[261].

Partendo da una qualificazione specifica dei *big data,* tali rientrerebbero tra le informazioni commerciali quali le liste clienti, i dati contrattuali, le informazioni circa i nominativi, i recapiti, le preferenze merceologiche o le abitudini di acquisto, tutte tipologie d'informazioni che la giurisprudenza italiana ha più volte affermato possano venir tutelati come segreti

---

[259] Si veda in tal senso G. MONDINI, *Big Data. Processi di big data analytics nelle imprese e nella P.A.: chi è proprietario dei dati?*, in *Quot. Giur*., 2019, 1. Si veda anche la sentenza del Trib. Torino, 6 luglio 2012, in *Giur. ann. dir. ind*., dove la giurisprudenza italiana ha confermato la valutazione del valore economico delle tecniche di marketing e di profilazione della clientela.

[260] Si veda in tal senso F. BANTERLE, M. BLEI, (nt. 255), 202.

[261] Così si è espresso G. BONELLI, *La tutela dei Big Data quale segreto Industriale,* in *Quot. Giur.*, 2019, 1.

commerciali[262]. Per l'applicazione della protezione risulta importante la valutazione del requisito di lecita acquisizione dei dati costituenti il *data set;* l'acquisto in malafede, o con colpa grave, delle informazioni escluderebbe infatti anche la tutelabilità come segreto commerciale, e questo comportamento è particolarmente rilevante nel settore dei *big data*, per la prassi diffusa di acquisizione di "pacchetti" di dati, che spesso avviene senza precauzioni, circa la loro legittima formazione e/o provenienza di questi.

Per ciò che concerne il requisito di segretezza, questo va inteso non in senso assoluto, bensì relativo, le informazioni inoltre possono essere protette non solo singolarmente ma anche "*nel loro insieme, o nella precisa configurazione e combinazione dei loro elementi*", ciò determina che possono venir tutelate informazioni in sé note o facilmente accessibili, ma che non siano, nel contempo conosciute o agevolmente conoscibili nel loro insieme o nella loro combinazione. Ciò rende potenzialmente idonei alla tutela come segreto commerciale tutti i dati derivanti dall'*Internet of Things***,** dai processi di *Machine to Machine,* a i sistemi di intelligenza artificiale, tecnologie che permettono la raccolta, oltre che l'elaborazione, di grandi volumi di informazioni in tempi ridotti[263].

Come stabilito dal n.2 dell'art. 98 c.p.i., l'informazione segreta deve avere un valore economico per essere tutelabile come segreto. Le attività di *data-driven economy* e i database a loro connessi consentono attività di "profilazione" di determinate categorie di soggetti e consumatori, sono capaci così di fornire alle imprese informazioni utili per un miglior svolgimento di certe attività o nell'ambito dell'offerta di servizi ai consumatori, acquisendo vantaggi competitivi nel mercato e più alti livelli di fidelizzazione dei clienti: il valore di tali dati è pertanto evidente.

Infine, sono necessarie delle misure di protezione adeguate per la protezione dei *big data* contro possibili attività di hackeraggio o boicottaggio interno. Abbiamo già presentato le numerose misure che l'impresa può implementare per tutelare le proprie informazioni in formato digitale (si veda *supra* 4.4.), anche attraverso il sistema *blockchain* (si veda *supra* 4.4.1.) o attraverso la stipula di NDA (si veda *supra* 3.3.1.). Sono quindi numerose le alternative che l'impresa ha per conformarsi al requisito n.3 dell'art. 98 c.p.i. anche

---

[262] Come indicato da F. BANTERLE, M. BLEI, (nt. 255), 5. Si veda anche la sentenza Trib. Bologna, 8 marzo 2011, in *DeJure* o la sentenza del Trib. Venezia, 16 luglio 2015, in *DeJure*.

[263] Cfr. G. OLIVI, *Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti, in Dir. ind*., 2020, II, 181.

nell'ambito di protezione dei *big data*[264].

Il capitale connesso ai *big data* può essere ulteriormente tutelato dall'art. 2598, co. 1, n.3, c.c., che ricordiamo vieta l'utilizzo di qualsiasi "*mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda"*; detta disciplina, come già indicato, è stata spesso applicata dalle Corti italiane per la tutela del segreto e che potrà dunque cumularsi anche nel caso dei *big data*[265].

Per concludere, la rivoluzione tecnologica in atto sta incidendo profondamente tanto sulla quotidianità dei singoli cittadini quanto sulle attività delle imprese. Il mutato contesto tecnologico consente infatti la datizzazione[266] di ogni fenomeno tramite la produzione, l'archiviazione e la conservazione di enormi moli di dati, realizzando la formazione del nuovo paradigma dei *big data* e con esso la possibilità di sviluppare attività di elaborazione su tali dati, grazie ad algoritmi e modelli di analisi, che permettono di svolgere indagini su larga scala, adottando strategie altamente personalizzate. I vantaggi connessi alle attività di *big data analysis* sono dunque molteplici e "seducenti", sia per soggetti pubblici e imprese, che possono così acquisire un vantaggio competitivo sul mercato, che per i singoli individui, i quali possono così usufruire di servizi su misura e personalizzati.

Il valore economico di questi beni immateriali non è rappresentato in realtà dal loro solo possesso, bensì dalla capacità di elaborarli efficacemente in modo tale da valorizzarne il potere informativo e generare nuova conoscenza. Ed è proprio il risultato di queste attività e il loro completo processo che può venir pienamente tutelato attraverso l'istituto del segreto commerciale. La tutela gioca un ruolo fondamentale nello sviluppo quantitativo e qualitativo dei processi sui dati in possesso delle imprese (ma anche della pubblica amministrazione), garantendone parallelamente sicurezza e un certo ritorno economico, grazie alle capacità e alle nuove conoscenze che verranno implementare attraverso l'elaborazione dei dati, capacità che permetteranno di condurre processi decisionali incisivi sulla base di dati oggettivi[267].

---

[264] Si veda G. BONELLI, (nt. 261), 1 ss. Come precisato da G. OLIVI, (nt. 263), 182, dall'elaborazione di dati non personali tramite i sistemi di intelligenza artificiale potrebbero ricavarsi però dati personali, inerenti ad esempio comportamenti e abitudini di vita e di consumo degli interessati, arrivando dunque ad effettuare attività di vera e propria profilazione, originariamente non prevista dal titolare.

[265] Si veda in tal senso G. BONELLI, (nt. 261), 3.

[266] Per datizzazione s'intende la tendenza a convertire un fenomeno in forma quantitativa o in dato, in modo da poterlo raccogliere, tabulare ed analizzare, come indicato da A. MORETTI, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Dir. inform*, 2018, 812.

[267] I vantaggi dei *big data* e delle attività connesse sono indicate da A. MORETTI, (nt. 266), 799 ss.

4.8. Industria 4.0 e segreti commerciali

Nel paradigma industriale 4.0 le tecnologie digitali svolgono una funzione di primaria importanza, permettendo l'implementazione di industrie sempre più iperconnesse e automatizzate, accompagnando le imprese nel processo di innovazione tecnologica e di sostenibilità ambientale, creando nuovi modelli di business e aumentando la produttività e la qualità degli impianti di produzione.

L'industria 4.0, e i piani governativi in materia, hanno fortemente beneficiato dello sviluppo del settore digitale, la digitalizzazione ha infatti reso possibile un maggior utilizzo di dati da parte delle imprese inerenti alle fasi produttive, l'ulteriore crescita della potenza di calcolo e della connettività degli strumenti e dei macchinari industriali hanno consentito l'evolversi di fenomeni quali *big data*, *l'open data,* l'internet delle cose*,* il *machine-to-machine* e il *cloud computing,* tecnologie che permettono la generazione di informazioni e la loro conservazione centralizzata all'interno dell'impresa. Le informazioni prodotte attraverso questi processi sono poi analizzate tramite strumenti digitali; le imprese possono così estrapolare un valore effettivo dai dati ottenuti, conseguendo vantaggi competitivi, e acquisendo, ad esempio, conoscenze tecniche relative a metodi e processi produttivi. Lo sviluppo del settore digitale ha permesso inoltre una maggiore interazione tra uomo e macchina, elemento fondamentale e caratteristico delle industrie 4.0, ha dato poi l'*input* per la crescita di nuove tipologie di imprese e di nuovi business, come nel ramo della stampa 3D, della robotica e delle iterazioni *machine-machine*[268].

Nelle imprese 4.0 le informazioni, i dati e i contenuti digitali concernenti la produzione, l'automatizzazione dei macchinari, ma anche le liste clienti e fornitori, costituiscono tra i principali capitali del patrimonio sociale, e sono fondamentali per assicurare efficienti processi produttivi e il funzionamento della rete stessa. Diventa quindi necessario per le imprese prevedere tutele specifiche e protezioni per questi asset strategici, contro una loro possibile illecita acquisizione, utilizzazione e divulgazione, che potrebbe compromettere

---

[268] Si veda in tal senso L. MACI, in *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare,* NetworkDigital360, reperibile in internet al seguente indirizzo: https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare/ 2021. Si definisce anche come quarta rivoluzione industriale, processo che porterà ad una produzione industriale del tutto automatizzata e interconnessa. Il termine Industria 4.0 è stata usato per la prima volta durante la Fiera di Hannover, in Germania, nel 2011.

l'intero sistema 4.0[269]. Tutti questi dati e informazioni possono ben integrare un segreto commerciale, essendo informazioni di natura tecnico-commerciale, riservate e con un certo valore economico per l'impresa, valore appunto dato dal trattamento confidenziale al quale sono sottoposte e dalla loro funzione all'interno dell'organizzazione produttiva[270].

Abbiamo già evidenziato come nel modello d'impresa 4.0 l'integrazione e l'interconessione di dati e informazioni tra i vari sistemi produttivi sono attività centrali per l'automatizzazione industriale. I vari componenti e macchinari dei sistemi produttivi sono infatti interconnessi tra loro, è dunque necessario per le imprese 4.0 garantire l'integrazione dei sistemi con un flusso costante di dati sia all'interno, che verso l'esterno, ma al contempo l'impresa dovrà assicurare che questi flussi di informazioni non comportino la perdita dello stato di riservatezza delle informazioni stesse, ciò infatti determinerebbe conseguenze fortemente negative per l'organizzazione stessa, con la possibile perdita dei vantaggi competitivi connessi al know-how riservato, maggiore sarà inoltre il flusso di informazioni circolante nell'impresa 4.0 maggiori saranno anche i rischi derivanti da possibili acquisizioni illecite. Ed è dunque essenziale per queste tipologie di imprese prevedere delle tutele specifiche a queste informazioni e conoscenze specifiche, applicando strumenti adeguati e un monitoraggio costante delle informazioni; tutto ciò può rientrare nella sfera di tutela specifica prevista dal segreto commerciale.

La trasformazione digitale ha comportato una serie di cambiamenti drastici, permettendo un miglioramento e una maggiore efficienza dei processi produttivi. In questo scenario di forte evoluzione i concetti di integrazione e di interconnessione sono alla base dell'innovazione per le imprese 4.0: è così divenuta ancora più attuale l'esigenza di garantire che il know-how e le informazioni dell'impresa siano correttamente tutelate e protette, essendo alla base del valore dell'innovazione. E il segreto commerciale è uno degli strumenti più adatti a svolgere questa importante funzione. Le imprese 4.0 potranno così innovare prodotti, processi e

---

[269] Come indicato da M. CUPOLO, in *Come tutelare know how e segreti commerciali nell'impresa 4.0,* RiskManagement360, 2020, reperibile in internet al seguente indirizzo: https://www.riskmanagement360.it/analisti-ed-esperti/come-tutelare-know-how-e-segreti-commerciali-nellimpresa-4-0/. Si veda anche V. FALCE, (nt. 26), 155, in cui si definisce dati e informazioni come: "Il motore, l'olio o anche la moneta dell'industria 4.0".

[270] Si veda in tal senso l'articolo di V. PANZIRONI, *Per i nuovi dati arriva la sfida di nuove regole*, IlSole24Ore, 2016, 21. Il Max Planck Institute, una delle principali istituzioni tedesche nel campo della ricerca di base, nel corso del Digital single market strategy 2016, promosso dalla Commissione Europea, si è schierato con forza contro l'introduzione di nuove forme di tutela nella prospettiva del diritto industriale**,** sostenendo che esistessero già degli strumenti di protezioni dei dati utilizzati dalle industrie 4.0, come ad esempio il segreto commerciale. Gli stessi dati, entro certi limiti, possono godere della tutela riconosciuta alle banche dati e, in casi limitati possono accedere anche alla tutela brevettuale, se soluzioni originali ad un problema tecnico.

servizi, creando parallelamente valore anche attraverso la tutela, la gestione, il monitoraggio costante dei dati e delle informazioni inerenti al know-how, attraverso la protezione offerta dall'istituto del segreto commerciale, capace di garantire una tutela flessibile e strutturata alle esigenze delle imprese 4.0[271].

4.9. Intelligenza artificiale e diritti di proprietà industriale

Per intelligenza artificiale (da ora IA) s'intendono tutti quei sistemi tecnologici capaci di compiere comportamenti intelligenti in autonomia attraverso l'analisi dell'ambiente per raggiungere specifici obiettivi. I sistemi di IA possono essere dei software che agiscono nel mondo virtuale, come assistenti vocali, motori di ricerca, sistemi di riconoscimento facciale, oppure un'incorporazione dei dispositivi hardware, come in robot avanzati, auto a guida autonoma, droni o applicazioni all'Internet delle cose[272].

Le tecnologie di IA necessitano di un gran quantitativo di dati per elaborare risultati e raggiungere un buon livello prestazionale, per questo il legame con lo sviluppo dei *big data* è molto forte; altre tematiche strettamente connesse alla tecnologia dell'IA sono il *machine learning* e il *cloud super-computing*, le quali hanno permesso un aumento progressivo della potenza di calcolo e dell'analisi di dati. L'IA è divenuta così la vera sfida strategica del 21esimo secolo, i passi in avanti effettuati dalla tecnologia sono stati notevoli e i processi di digitalizzazione sono fenomeni complementari allo sviluppo dell'IA, consentendo l'evoluzione della tecnologia come mai prima. I sistemi di IA sono in grado oggi di effettuare attività che da sempre erano ritenute di esclusivo appannaggio degli esseri umani, come redigere articoli, tradurre testi, dipingere opere d'arte, ideare soluzioni a problemi tecnici, ma i possibili campi d'applicazione sono numerosi e aumenteranno ulteriormente nel futuro[273]. Parallelamente allo sviluppo dell'IA è emersa la questione della regolamentazione della stessa, sia in tema di responsabilità civile, sia per gli aspetti etici connessi; si è poi resa necessaria una regolamentazione specifica dei diritti di proprietà intellettuale per lo sviluppo di tecnologie di IA e per la tutela delle produzioni generate dall'IA.

---

271 Così si è anche espressa anche M. CUPOLO, *Industria 4.0, l'importanza di know how e segreti commerciali,* Industry4business, 2020, reperibile in internet al seguente indirizzo: https://www.industry4business.it/esperti-e-analisti/industria-4-0-limportanza-di-know-how-e-segreti-commerciali/.

272 La definizione di IA è stata estrapolata da F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 193.

273 Si veda G. SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, in *Dir. ind*, 2019, IV, 253.

In tal senso il 20 ottobre 2020 il Parlamento Europeo ha adottato tre risoluzioni contenenti raccomandazioni in materia di regolamentazione dell'IA diretti alla Commissione Europea, questo in previsione della redazione e della stesura dei futuri regolamenti a livello comunitario, regolamenti che sono già comunque stati anticipati nel Libro bianco sull'IA pubblicato dalla stessa Commissione il 19 febbraio 2020. L'*iter* proseguirà con le proposte legislative che la Commissione stessa dovrebbe presentare nel corso del 2021. Nelle risoluzioni si è evidenziata la necessità di promuovere l'etica e lo sviluppo tecnologico dell'IA all'interno dell'Unione europea, tutelando parimenti i diritti di proprietà, definendo un quadro chiaro della materia, in particolare attraverso l'adozione di legislazioni uniformi in tutta l'Unione che tutelino pienamente sia i valori europei che i diritti dei cittadini in un'ottica di sviluppo tecnologico[274].

Particolarmente complesso però è il tema della proprietà intellettuale connesso all'IA. I robot o i computer dotati di IA sono in grado di realizzare trailer cinematografici, quadri o romanzi, tutte opere tutelabili ai sensi del diritto d'autore. Non provenendo però queste opere da esseri umani non è chiaro se possano essere tutelabili come diritti di proprietà intellettuale, così come non è chiaro a chi spetti la titolarità dell'opera e i diritti relativi ad essa. Il dibattito è fortemente attuale, poiché prima dell'avvento di queste tecnologie si riteneva che la proprietà del *copyright* potesse essere esclusivamente in capo ad una persona fisica, i computer o i programmi per elaboratore erano semplicemente elementi di supporto nel processo creativo mentre l'originalità dell'opera era sempre frutto dell'attività di esseri umani[275].

In Europa, la Corte di Giustizia Europea (CGUE) ha dichiarato in diverse sentenze che il

---

[274] In tal senso si veda V. COCCA, in *Responsabilità civile, etica e tutela dei diritti di proprietà intellettuale nei sistemi di intelligenza artificiale,* in *Quot. giur*, 2021, 1. Si vedano anche le risoluzioni del Parlamento europeo del 20 ottobre 2020 recanti raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, sul quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, e la relazione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale. In particolare il Parlamento ha evidenziato la necessità di prevedere che "la regolamentazione nel settore delle tecnologie di IA avvenga a livello di Unione; che un quadro normativo dell'Unione pienamente armonizzato nel settore dell'IA potrà diventare un riferimento legislativo a livello internazionale", evidenziando inoltre che "lo sviluppo dell'IA e delle tecnologie correlate porterà innovazione, ricerca, la mobilitazione di investimenti e considerevoli benefici economici, sociali, ambientali, pubblici e di sicurezza".

[275] Si veda F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 193. Il dibattito sulla questione è acceso a livello internazionale. Negli USA, ad esempio, l'Ufficio del *copyright* ha dichiarato che registrerà un'opera originale attribuendo la paternità a condizione che l'opera sia stata creata da un essere umano. Anche le legislazioni di Spagna e Germania disciplinano la materia in maniera analoga, ossia dichiarano che solo le opere create da un essere umano possono essere protette dal diritto d'autore. Per ciò risulta necessario prevedere, come evidenziato poc'anzi, un quadro normativo dell'Unione armonizzato, in quanto si registrano in materia delle sostanziali differenze tra le legislazioni nazionali.

copyright si applica solo ad opere che presentano elementi di originalità, dove l'originalità riflette la "*creazione intellettuale dell'autore*" e la sua personalità è "*risultato di un'attività dell'ingegno umano*": la presenza di un autore "umano" sembra quindi essere necessaria perché il lavoro possa essere tutelato con *copyright*[276]. Ricordiamo inoltre che la disciplina sul diritto d'autore prevede che il diritto all'utilizzo economico dell'opera perdura per tutta la vita dell'autore e sino a settant'anni dopo la sua morte (si veda *supra* 2.4.), il calcolo delle protezioni del diritto d'autore fanno perciò riferimento alla vita degli autori come persone fisiche, comportando delle difficoltà nella definizione della durata dei diritti connessi ad opere generate da soli sistemi di IA.

Nell'attesa di una disciplina ad *hoc* che colmi il vuoto normativo, in dottrina si riscontrano alcune proposte, tra queste una possibile equiparazione delle opere generate da "soggetti elettronici" alle "opere orfane", di cui al d.lgs. 10 novembre 2014, n.163. Si tratterebbe comunque di una soluzione temporanea, che richiederebbe un'interpretazione estensiva della normativa fino a quando, a livello nazionale, e nell'UE, non venga disposta una disciplina specifica che individui i diritti connessi alle opere generate direttamente ed esclusivamente dalla IA[277].

Ulteriore questione sorge nel definire le possibili protezioni giuridiche applicabili alle idee generate da computer programmati con IA: tali sistemi sono infatti in grado di realizzare delle vere e proprie invenzioni brevettabili, definibili come "*computer generated*" cioè prodotte da un computer senza l'identificazione di un inventore umano[278].

Le tecnologie di IA si baserebbero su modelli computazionali e algoritmi, considerati metodi matematici e dunque non brevettabili, come stabilito dall'art. 45, co. 4, c.p.i. (si veda *supra* 2.1.) e dalla Convenzione di Monaco. È però necessario evidenziare che questo limite è posto solamente per le invenzioni generate autonomamente dall'IA, cioè le c.d. invenzioni *computer generated*, mentre per le creazioni ottenute da un'inventore umano con la sola assistenza

---

276 In tal senso si veda l'art. 1 della direttiva del Consiglio 14 maggio 1991, 91/250/CEE, relativa alla tutela giuridica dei programmi per elaboratore, co. 3, in cui si recita che: "Un programma per elaboratore è tutelato se originale, ossia se è il risultato della creazione intellettuale dell'autore". Si veda inoltre la sentenza della Corte di Giustizia Europea sul caso Infopaq (C05/8 Infopaq), o le sentenze delle cause C403/08 e C429/08 denominate Football Association Premier League. Si veda inoltre F. SARZANA DI S. IPPOLITO, M. NICOTRA, (nt. 216), 243.

277 Come proposto da C. TREVISI, *La regolamentazione in materia di Intelligenza Artificiale, robot, automazione: a che punto siamo*, Medialaws, 2018, reperibile in internet al seguente indirizzo: http://www.medialaws.eu/la-regolamentazione-in-materia-di-intelligenza-artificiale-robot-automazione-a-che-punto-siamo/.

278 La definizione di invenzioni "*computer generated*" è rinvenibile in G. SENA, *Invenzioni brevettabili e intelligenza artificiale*, in *Dir. ind.*, 2020, II, 151.

dell'IA la tutela brevettuale è garantita.

Tra le questioni più complesse nei casi d'invenzioni generate esclusivamente dall'IA c'è quella della corretta individuazione del soggetto titolare dei diritti connessi al brevetto, come il diritto alla titolarità e alla paternità del brevetto. I sistemi di IA non sarebbero infatti soggetti dotati di capacità giuridica, non essendo né persone fisiche né giuridiche, e non avrebbero dunque il diritto a risultare come titolari del brevetto, in quanto questo, o un qualsiasi altro diritto soggettivo, richiede l'identificazione di uno specifico soggetto giuridico. Le discipline nazionale ed europea prevedono che i diritti connessi al brevetto possano appartenere a un soggetto diverso dall'inventore, ossia a quello che è definito come "imprenditore della ricerca", cioè a colui che promuove, organizza, finanzia ed in genere sopporta i costi ed i rischi economici dell'invenzione, come avviene nelle c.d. invenzioni del dipendente e nei contratti di ricerca. Le invenzioni *computer generated* potrebbero dunque essere brevettabili dall'imprenditore della ricerca, ossia da parte del soggetto che dispone del sistema di IA, acquisendo così i diritti di titolarità derivanti dal brevetto[279].

Diverso è il tema del c.d. diritto morale, ossia il riconoscimento della paternità dell'invenzione, che spetterebbe unicamente all'inventore, inventore che dovrebbe venir identificato nella domanda di brevetto. In questo caso le norme richiedono espressamente che l'inventore designato sia una persona fisica, escludendo quindi la possibilità che un sistema di IA possa acquisire la paternità dell'invenzione. In tal senso proprio nell'agosto 2019 l'EPO ha rifiutato il deposito di due brevetti internazionali per "invenzioni generate dall'IA", ossia di invenzioni generate autonomamente da un'IA senza l'ausilio o il supporto di nessuna persona fisica che possa ritenersi inventore. L'EPO, rifiutando l'istanza di deposito, ha chiarito che la scelta evidenzia la necessità che nel brevetto sia previsto un'inventore rappresentante una persona fisica e non una macchina, in quanto la designazione di una macchina come inventore non soddisferebbe i requisiti legali disposti dalla Convenzione sul Brevetto Europeo (EPC)[280].

---

[279] In tal senso si è espresso G. SENA, (nt. 278), 155. Si veda anche l'art. 58 della Convenzione sul Brevetto Europeo in cui si stabilisce che "ogni persona fisica o giuridica ed ogni società assimilata ad una persona giuridica può richiedere un brevetto europeo".

[280] Si vedano le domande di brevettazione EP 18 275 163 ed EP 18 275 174. In entrambe le applicazioni una macchina chiamata "DABUS" viene descritta come "*a type of connectionist artificial intelligence*" ed è definita come inventore. Il richiedente ha affermato di aver acquisito il diritto al brevetto europeo dall'inventore in qualità di successore del titolo, sostenendo che, in quanto proprietario della macchina, gli sono stati assegnati i diritti di proprietà intellettuale creati da questa macchina. Si veda in tal senso l'articolo pubblicato nel sito ufficiale dell'EPO, *EPO publishes grounds for its decision to refuse two patent applications naming a machine as inventor*, 2020, reperibile in internet al seguente indirizzo: https://www.epo.org/news-events/news/2020/20200128.html. Si veda anche G. SENA, (nt. 278), 158.

L'interazione tra IA, diritto d'autore e brevetto pone insomma nuove sfide a livello regolatorio e in questo contesto ancora non del tutto chiaro il segreto commerciale può risultare uno strumento fondamentale per la tutela dei risultati inventivi dell'IA: in attesa di una più chiara regolamentazione in materia, le imprese potrebbero infatti mantenere le idee e le opere *computer generated* segrete, tutelando il loro valore attraverso l'istituto del segreto commerciale, evitando così che le stesse tecnologie, le informazioni e le conoscenze generate dall'IA siano acquisite da soggetti esterni all'organizzazione, pregiudicandone la possibile successiva tutela attraverso il diritto d'autore o la protezione brevettuale. A parere di chi scrive il segreto commerciale si delinea dunque come una potenziale misura temporanea, sebbene del tutto valida, in previsione di una regolamentazione specifica in materia di IA e di protezione dei diritti di proprietà intellettuale[281].

4.10. Risvolti pratici per le imprese digitali

Abbiamo analizzato le principali misure di protezione per la tutela di segreti commerciali attraverso le tecnologie digitali oggi disponibili, ad esempio il sistema *blockchain;* si sono poi descritte le normative che hanno avuto un impatto più significativo nella determinazione della tutela del know-how segreto dell'impresa, dal GDPR alla direttiva NIS, e come la tutela dei segreti commerciali si applichi opportunamente ad attività strettamente digitali, come nell'analisi dei *big data*, l'implementazione dell'industria 4.0 e l'IA.

In questo elaborato si è più volte affermata la centralità del mondo digitale nell'economia moderna: non c'è settore che non utilizzi sistemi tecnologici come microchip, software, *firmware*, *cloud*, *big data,* standard essenziali, *patent pools* etc, ed è quindi fondamentale che le imprese digitali sviluppino un approccio strategico che preveda la tutela delle loro informazioni, del loro specifico know-how e, più in generale, della loro proprietà intellettuale. Il segreto commerciale risponde in maniera efficiente a queste esigenze: molte sono infatti le imprese digitali che scelgono di tutelare le proprie conoscenze, come gli asset digitali, attraverso il segreto commerciale, costruendo così una prima "linea di difesa". Sebbene non sia richiesta nessuna domanda o registrazione, è fondamentale essere attenti nel proteggere efficacemente le informazioni, e questo potrebbe risultare un processo non meno banale della

[281] La possibile applicazione del segreto commerciale come misura alternativa di tutela è indicata anche da G. SPEDICATO, (nt. 273), 300.

costituzione di altri titoli giuridici che invece richiedono l'approvazione da parte di un organo responsabile, come nel caso dei brevetti[282].

Tuttavia la sola applicazione dell'istituto non può bastare, perché le imprese, sia digitali, ma anche quelle attive nei settori più tradizionali, hanno necessità di investire in strategie che permettano una piena tutela delle loro informazioni: ad esempio, nel caso di illecita acquisizione delle proprie conoscenze riservate, l'impresa dovrà essere in grado di dimostrare, durante il processo, l'esistenza di un diritto specifico su tale asset immateriale e l'adeguatezza delle misure applicate come richiesto specificatamente dalla legge, presentando la documentazione necessaria e le prove dell'eventuale abuso subito. Se l'impresa non riuscisse a dimostrare ciò, la privativa avrebbe l'esclusivo effetto di limitare possibili acquisizioni illecite, in un ruolo prettamente "difensivo", ma non permetterebbe al titolare del segreto di ottenere un risarcimento del danno subito in forma consistente o la concessione di azioni inibitorie capaci di limitare i danni conseguenti da un'acquisizione, un utilizzo, o una comunicazione illecita delle proprie conoscenze mantenute segrete; le imprese devono dunque prepararsi alla possibilità più remota di subire un abuso, adattando strategie reattive e resilienti in questo senso.

L'applicazione della tutela dell'informazione come segreto commerciale non ha effetti e benefici solo per l'informazione tutelata, bensì ha delle ripercussioni sul complesso dell'attività dell'impresa. Lo stesso processo di costituzione del segreto costituisce una strategia con impatti notevoli sull'intera organizzazione: abbiamo già visto come il management, nelle fasi di costituzione del segreto, dovrà selezionare gli strumenti endoaziendali e esoaziendali più adeguati al caso specifico, determinando inoltre verso quali soggetti applicare queste misure. Sarà quindi necessario un monitoraggio costante delle informazioni segrete, così da assicurarne una protezione adeguata. Il processo di costituzione necessita perciò di una strategia applicativa che va sviluppata e implementata nel corso del tempo, e ciò può richiedere investimenti di tempo e denaro, anche notevoli.

L'utilizzo della tutela delle informazioni come segreto commerciale può avere effetti significativi anche a livello gestionale all'interno dell'impresa, si pensi ad esempio

---

[282] Come indicato da F. CHIEZZI, *La tutela del know-how nell'era digitale*, Le Fonti Legal, 2018, reperibile in internet al seguente indirizzo: https://www.lefonti.legal/la-tutela-del-know-how-nellera-digitale/. Questi settori sono più scevri dalla cultura brevettuale, l'immediato e attuale incontro tra il mondo dell'industria tradizionale e delle tecnologie avanzate comporterà dei rischi di azioni giudiziali di inibitoria e rilevanti risarcimento dei danni. È dunque, per l'autrice, essenziale che anche le imprese digitali adottino al più presto presidi di controllo per una corretta attività di brevettazione delle proprie invenzioni o di tutela della proprietà intellettuale.

all'adeguamento nella propria organizzazione di sistemi organizzativi definibili di "*zero-trust*": il processo prevedrebbe l'archiviazione delle informazioni in un deposito virtuale, l'accesso al deposito dovrebbe essere disposto al minor numero possibile di utenti, con l'utilizzazione di autenticazione a due fattori e un monitoraggio e una registrazione costante degli accessi[283]. Il sistema gestionale dell'impresa sarebbe così idoneo a garantire la segretezza dell'informazione, ma ciò potrebbe comportare l'applicazione di importanti misure gestionali che non sarebbero invece richieste in realtà sprovviste di segreti commerciali[284].

Ulteriori conseguenze, a livello pratico, sono dettate dal fatto che nelle imprese titolari di segreti commerciali è preferibile la costituzione di *team* di piccole dimensioni, questo in un'ottica di una maggiore tutela della segretezza delle informazioni: in altre parole, l'impresa determinerà chi ha davvero necessità di avere una conoscenza diretta del know-how o dell'informazione segreta per l'esercizio delle proprie mansioni, limitandone quanto più possibile la diffusione.

Per applicare la tutela come segreto commerciale alle informazioni l'impresa deve inoltre modificare i rapporti con i propri dipendenti e fornitori: come abbiamo già illustrato, è necessario prevedere la sottoscrizione di NDA sia con dipendenti, che con terzi soggetti con cui l'impresa mantiene relazioni, per limitare possibili utilizzi illeciti del proprio know-how e delle proprie informazioni segrete[285].

La stessa scelta di tutelare l'informazione come segreto commerciale invece che con altri diritti di proprietà intellettuale è una scelta prettamente strategica; scelta che è stata attuata da grandi realtà, come nel caso di Google, per la tutela dei propri algoritmi.

I motori di ricerca sono al giorno d'oggi essenziali per la ricerca di notizie e informazioni, siano essi di natura commerciale, scientifica o culturale. Google risulta il primo motore di ricerca al mondo come quota di mercato, con la sola e significativa eccezione della Cina, dove Baidu, campione nazionale cinese, è in prima posizione per quota di mercato. Presentando

---

[283] Queste sono solamente alcune delle misure che potrebbero venir messe in pratica dall'impresa, per una analisi più dettagliata delle possibili misure sia endoaziendali che esoaziendali. Si veda *supra* il capitolo 3.

[284] Il sistema "*zero-trust"* è presentato da DOUG CAHILL, vicepresidente e direttore del gruppo di sicurezza informatica presso Enterprise Strategy Group, in *Come proteggere gli algoritmi dal furto di proprietà intellettuale,* CIO Business Technology Leadership, 2020, reperibile in internet al seguente indirizzo: https://www.cwi.it/cio/come-proteggere-gli-algoritmi-dal-furto-di-proprieta-intellettuale_42129810.

[285] L'importanza della sottoscrizione dei NDA per la tutela di segreti commerciali è sottolineata anche da MARY HILDEBRAND, presidente e responsabile di privacy e sicurezza informatica di Lowenstein Sandler, in CIO*,* (nt. 284).

brevemente il sistema su cui si basa l'attività dei motori di ricerca, che esula dall'argomento di questo elaborato, questo permette l'accesso ad una serie di siti internet collegati ad una parola chiave selezionata dall'utente. L'algoritmo di Google fornisce dunque una serie di risultati, allineandoli in ordine di rilevanza in base a diversi fattori, come il numero di *link* che rimandano a quel sito o al numero di visitatori: quest'opera automatizzata viene alimentata da *bot* o *crawler,* che perlustrando instancabilmente la rete, rilevano e collocano in una griglia di riferimento (la c.d. indicizzazione) i contenuti di tutti i siti presenti nella rete internet[286].

Google ha deciso di mantenere proprio l'algoritmo su cui si basa tutta l'attività del motore di ricerca tutelandolo come segreto industriale e ripetutamente perfezionandolo. L'indicizzazione è infatti frutto di funzionalità create dal proprio software, che viene attivato secondo certi algoritmi coperti dal segreto industriale. La stessa Google afferma che il motore di ricerca viene attivato attraverso il software denominato "spider", il quale opera scandagliando il web, fotocopiando e immagazzinando le pagine prodotte dai siti sorgente. La fase di indicizzazione, i cui risultati sono fondamentali per i proprietari delle pagine web in quanto un miglior posizionamento nei primi risultati permette all'unisono un maggior traffico all'interno del proprio sito, e quindi maggiori contatti e vendite, è retto da un algoritmo molto complesso che permette l'associazione delle chiavi di ricerca proposte dagli utenti con le pagine web memorizzate sulla base di parametri predeterminati, in base alla composizione dell'algoritmo stesso, e ciò viene applicato anche al ranking delle URL che appaiono a seguito della indicizzazione dei termini chiave[287].

L'importanza e la solidità della protezione offerta dal segreto commerciale è quindi confermata da questo caso, che riguarda una delle società più grandi al mondo e sicuramente leader nel settore digitale com'è Google, la quale ha optato per proteggere l'algoritmo alla base dell'indicizzazione, un suo asset di considerevole importanza, attraverso l'istituto del segreto industriale. Ciò è la dimostrazione del fatto che questo istituto può avere una importante applicazione pratica in particolare nel settore digitale, essendo proprio le caratteristiche intrinseche della disciplina del segreto commerciale a permettere una flessibilità della tutela che, come indicato nei paragrafi precedenti, riesce a ben adattarsi alle

---

[286] In tal senso si veda Corte Giust. UE, 23 marzo 2010, n. 238, in *Giur. It*., 2010, 7, 1603 e M. RICOLFI, *Motori di ricerca, link sponsorizzati e diritto dei marchi: il caso Google di fronte alla corte di giustizia,* in *Inf. giur. e dir. dell'inf*., 2014.

[287] Come indicato nella sentenza del Trib. Milano, sez. I, 24 gennaio 2020, n. 4911, in *DeJure*.

esigenze di un settore in forte evoluzione com'è quello digitale, per la protezione del know-how e delle informazioni inerenti, ad esempio, al codice sorgente dei software, agli algoritmi, ad invenzioni generate dall'IA o ai risultati rinvenuti dall'analisi di *big data,* non escludendo comunque ulteriori e diverse applicazioni[288].

[288] In tal senso si è espresso G. BONELLI, (nt. 261), 2 presentando i diversi vantaggi della tutela del segreto.

CAPITOLO 5. RIFLESSIONI CONCLUSIVE SU FUTURE EVOLUZIONI

Questo elaborato è stato sviluppato con lo scopo specifico di porre in evidenza come la disciplina dei segreti commerciali sia adeguata alla protezione degli asset immateriali nell'economia digitale. Sebbene la disciplina possa applicarsi a qualsiasi informazioni di natura tecnico-commerciale, in ogni tipologia di impresa, le caratteristiche intrinseche dell'istituto del segreto gli permettono di costituire una forma di tutela efficiente al know-how, in particolar modo nelle c.d. imprese digitali, attraverso procedimenti che risultano semplici ed efficienti.

Il processo di costituzione della tutela deve però seguire una certa logica, l'imprenditore, sia che esso operi in un settore digitale, che in un settore più tradizionale, dev'essere certo di rispettare pienamente quelli che sono i requisiti minimi richiesti dalla legge per assicurarsi la tutela in caso di acquisizione, utilizzo o divulgazione illecita di informazioni segrete da parte di terzi. Dovrà quindi applicare misure ragionevolmente adeguate ai propri segreti commerciali, garantendo la piena riservatezza e il valore economico delle proprie conoscenze. E gli strumenti digitali offrono in tal senso forme di protezione conformi alle disposizioni di legge, valide alternative ai sistemi classici di conservazioni di segreti, come possono essere casseforti, cassette di sicurezza, o il sistema notarile.

L'utilizzo di diritti di proprietà intellettuale è diventato oramai imprescindibile per tutte quelle attività economiche che vogliono garantirsi un ritorno economico dalle proprie attività innovative, grazie alla duplice possibilità, offerta dai diversi istituti, di appropriarsi dei benefici economici che derivano dalle innovazioni, senza pregiudicare parallelamente i rapporti con i soggetti esterni all'organizzazione, anzi sviluppandoli ulteriormente, in un'ottica di piena collaborazione e di innovazione "aperta", in un sistema che funge da catalizzatore per la generazione di nuove idee, permettendo così una migliore risposta da parte delle imprese a quelle che sono le esigenze dei consumatori e alle sfide poste dalla società e dal mercato nel suo complesso. Le pratiche di innovazione aperta sarebbero dunque correlate positivamente con l'utilizzo di diritti di proprietà intellettuale, questo per mantenere e aumentare la competitività delle innovazioni introdotte. In particolare, l'uso di segreti commerciali aumenterebbe significativamente nei casi di relazione con partner commerciali

geograficamente distanti: risulta infatti che le imprese che collaborano con società o enti in Cina, USA o India tendono a conservare maggiori informazioni come segreti commerciali[289].

Il prezioso patrimonio imprenditoriale costituito da informazioni e know-how forma infatti il vero "DNA" delle organizzazioni economiche, permettendone una differenziazione in mercati sempre più competitivi, ed è dunque sempre più necessario preservare il valore di questi capitali. Sebbene i mezzi per far ciò possano essere diversi, dato che le imprese hanno la possibilità di usufruire di tutele specifiche tramite brevetti, disegni e modelli, modelli d'utilità o diritto d'autore, il segreto commerciale si afferma come disciplina idonea a proteggere il patrimonio di informazioni e conoscenze in mercati soggetti a rapide evoluzioni e cambiamenti, caratterizzati da relazioni economico-commerciali tra operatori diversi a livello globale, come si presentano i mercati moderni, in particolar modo nel settore digitale[290].

Alcune imprese attribuiscono già ai segreti commerciali un ruolo di primaria importanza, e Google ne rappresenta un caso emblematico. Queste realtà sfruttano la riservatezza del know-how come strumento per affermare la competitività commerciale attraverso la salvaguardia delle capacità di gestione dell'innovazione nel medio e lungo periodo. La stessa Commissione Europea nel 2011 ha promosso uno studio sul segreto commerciale e sulle informazioni commerciali riservate nel mercato europeo, pubblicando poi, nel gennaio 2012, un report. Da tale studio è risultato che su un campione di 537 società con sede in Europa, tra le quali 323 PMI, il 75% ritiene il segreto industriale un asset strategicamente rilevante per la crescita, per la competitività e la crescita delle *performance* commerciali, mentre il 39% degli intervistati ha espresso preoccupazione sulle conseguenze derivanti dalla perdita di segreti o dalla caduta in pubblico dominio delle informazioni sottoposte a trattamenti di natura confidenziale[291].

Le PMI, in particolare, richiedono una maggiore diffusione della conoscenza per lo sviluppo di opportunità dinamiche ma, al contempo, anche di discipline specifiche per la protezione e lo scambio di conoscenze, specialmente nel contesto delle attività di ricerca e sviluppo e

---

289 Si veda in tal senso EUIPO, (nt. 113), 52, dove si parla di "paradosso dell'apertura": mentre la creazione di innovazioni spesso richiede apertura, la loro commercializzazione richiederebbe una maggiore protezione.

290 Come indicato nella tabella A in appendice, i segreti commerciali risultano il terzo metodo di protezione delle innovazione in Europa, con una media comunitaria al 52,3%, prima di altri diritti di proprietà come marchi (41%), brevetti (31,7%) e diritti d'autore (27,4%).

291 Il Rapporto è disponibile presso il sito: https://ec.europa.eu/growth/industry/policy/intellectual-property/trade-secrets_en. Tale posizione è condivisa da D.S. ALMELING, *Seven Reasons Why Trade Secrets Are Increasingly Important*, in *Berkeley Technological Law Journal*, 2012, XXVII, 1091. Si veda anche V. FALCE, (nt. 22), 135.

dell'innovazione. Tuttavia, tra i maggiori limiti rinvenibili nella disciplina del segreto commerciale, si evidenzia certamente la bassa conoscenza della materia e delle possibilità collegate alla tutela delle informazioni come segreti commerciali da parte del consumatore-imprenditore, in particolar modo proprio nelle realtà delle PMI italiane, come dimostrano i dati in appendice: solo il 22,6% delle PMI italiane utilizzerebbe segreti commerciali per tutelare le proprie innovazioni, rispetto alla media europea che si attesta al 51,2%[292]. Questo non permette una diffusione dell'istituto e una sua piena e ottimale utilizzazione, sarebbe dunque necessaria un'opera di vera e propria sensibilizzazione, per incentivare l'impiego di adeguati strumenti di tutela capaci di valorizzare il contenuto del know-how nelle imprese, ciò potrebbe realizzarsi tramite attività di vero e proprio marketing per la promozione e la diffusione dell'istituto nelle PMI. Da questa prospettiva quindi il segreto commerciale può essere indicato come un possibile fattore di progresso, in quanto strumento capace di stimolare processi di innovazione e di collaborazione, espressione della libertà di iniziativa economica dell'imprenditore, principio costituzionalmente garantito all'articolo 41.

In contrapposizione a questa considerazione, i segreti commerciali possono ritenersi figli dell'estensione in senso protezionistico della tutela offerta dai diritti di proprietà intellettuale: la disciplina del segreto si sovrappone infatti ad altri istituti, proponendosi, ad esempio, come valida alternativa al modello classico della brevettazione di invenzioni. Vi è però il rischio che la tutela disposta dai segreti commerciali limiti in qualche maniera la libertà di iniziativa economica degli operatori concorrenti, generando una situazione di conflitto tra proprietà intellettuale e diritto *antitrust*. Il segreto deve quindi rappresentare un "motore" sano della competizione, remunerando gli investimenti effettuati dalle imprese, sostenendo i processi di innovazione attraverso la protezione della riservatezza delle invenzioni e delle conoscenze.

L'analisi focalizzata in questo testo sullo specifico settore digitale non è causale. Sebbene in qualsiasi attività economica possa essere riscontrata una qualche forma di segretezza delle informazioni (si pensi ad esempio ad una ricetta segreta di un ristorante oppure a particolari metodi di lavorazione di un'officina meccanica), le opportunità economiche offerte dalla digitalizzazione e dai settori high tech sono molteplici: dagli ultimi studi risulta che nei prossimi anni 9 lavori su 10 richiederanno competenze digitali, mentre il 70% del valore

[292] Si veda in tal senso la tabella B e i grafici C in appendice.

economico sarà generato nelle piattaforme digitali[293]. Parallelamente alla crescita dell'importanza del settore digitale sarà sempre più necessario garantire la sicurezza informatica, la protezione dei dati, la difesa da attacchi esterni, controllando con regolarità le operazioni informatiche. La criminalità digitale rischia infatti di provocare danni spesso irrimediabili, compromettendo lo stesso processo di digitalizzazione, e le minacce di pratiche fraudolente stanno aumentando con il progredire della digitalizzazione delle attività economiche. In Italia, secondo gli studi di settore, le PMI rappresenterebbero il bersaglio preferito degli hacker: il 71% di tutte le violazioni di dati e di informazioni, finalizzate principalmente all'acquisizione fraudolenta di conoscenze e di diritti di proprietà intellettuale, avrebbe proprio come destinatari imprese con meno di 100 dipendenti[294]. La disciplina del segreto commerciale può dunque avere un ruolo fondamentale nell'economia digitale del futuro, garantendo celermente protezioni e strumenti alle imprese per preservare i propri asset immateriali. Questo permetterà di garantire un futuro prospero a qualsiasi attività che decida di investire in innovazione digitale attraverso la tutela delle proprie conoscenze, fonte di vantaggi competitivi, in particolare per le PMI.

Le tematiche trattate nel presente lavoro come *big data*, industria 4.0, *cybersecurity*, intelligenza artificiale, *blockchain* stanno oramai acquisendo una rilevanza fondamentale nelle attività imprenditoriali, plasmando i metodi operativi e produttivi, ma anche le scelte dei consumatori. Abbiamo visto come la disciplina del segreto commerciale bene si integri con tutte queste tecnologie, permettendone ulteriori sviluppi e assicurandone la valorizzazione. Peraltro, la rivoluzione digitale in atto potrà offrire alle imprese anche altre e migliori possibilità, non si escludono quindi ulteriori applicazioni delle stesse alla disciplina del segreto in futuro.

È assai probabile però che saranno necessarie in futuro delle modifiche a livello normativo per adeguare il testo attuale all'evolversi dei mercati digitali e delle tecnologie. Come apportato recentemente dalla direttiva UE 2016/943 il segreto commerciale richiede norme comuni e omogenee in tutti gli Stati membri, in modo tale da limitare differenze che possano

---

293 Si veda in tal senso il rapporto della Commissione Europea, *The Digital Skills Gap,* reperibile in internet al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs. Si veda anche E. SALZA, *Opportunità della digitalizzazione e rischi di cybercrime,* IlSole24Ore, 2021.

294 Si veda in tal senso il report della Commissione Europea, *The scale and impact of industrial espionage and theft of trade secrets through cyber*, 2018, 33, reperibile in internet al seguente indirizzo: https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en.

pregiudicare il corretto funzionamento del mercato interno. L'Italia si è conformata alle disposizioni della suddetta direttiva modificando gli artt. 98, 99, 121, 124, 126 c.p.i. e 388, 623 c.p.; ma ciò potrebbe non bastare. Entro il 9 giugno 2021 l'EUIPO avrebbe dovuto elaborare una relazione preliminare sulle controversie relative all'acquisizione, utilizzo e divulgazione illeciti di segreti commerciali in applicazione della direttiva 2016/943, mentre la Commissione UE redigerà una valutazione d'impatto finale entro il 9 giugno 2026. L'EUIPO e la Commissione potrebbero dunque riscontrare il mancato o l'insufficiente recepimento di alcune disposizioni della direttiva anche da parte dell'Italia, in particolare in tema di applicazione dei metodi di valutazione in bilancio dei segreti commerciali e dei possibili sistemi di rivalutazione del segreto, che in Italia, secondo le disposizioni OIC 24, non si conformerebbero al sistema *faire value* ma alla sola applicazione del metodo del costo storico, disincentivando così l'utilizzo dell'istituto. L'UE potrebbe dunque emanare un regolamento europeo vincolante per tutti gli Stati membri, imponendo sistemi comuni di valutazione e rivalutazione dei segreti commerciali in bilancio, entrando così "a gamba tesa" sulla competenza normativa nazionale in materia. Ulteriormente a ciò, abbiamo già sottolineato come le tecnologie più moderne*,* ad esempio in tema di *blockchain* e IA, presentano dei vuoti normativi importanti, è dunque fondamentale che l'Italia agisca quanto prima per limitare la formazione di "zone grigie" che non permetterebbero un pieno progresso e l'impiego di queste tecnologie, anche nell'ambito della disciplina dei segreti commerciali.

Concludendo, sebbene i segreti commerciali esistano da secoli, la loro operatività rimane ad oggi fondamentale per preservare il patrimonio informativo e il know-how delle imprese, con funzioni tutelative della proprietà intellettuale, per la promozione di una corretta concorrenza e lo sviluppo di processi di innovazione aperta, tematiche che risultano più che mai attuali. Non si esclude però che in un futuro prossimo, sempre più digitale, i segreti commerciali acquisiscano ancora maggior valore, anche attraverso modifiche normative e una loro promozione nella concreta realtà delle PMI, permettendo così alla disciplina del segreto commerciale di esprimere tutto il suo potenziale e di giocare un ruolo di prim'ordine nel sostenere e proteggere l'evoluzione dell'economia della conoscenza e dell'innovazione.

APPENDICE

A. Tabella esplicativa dei sistemi di protezione delle innovazioni di prodotto o di processo delle imprese in UE, 2010-2012

Country	Lead Time Advantages	Complexity of Good / Services	Trade Secrets	Trade Marks	Patents	Copyright	Design Registration
AT	84.3 %	82.6 %	64.8 %	53.4 %	35.3 %	34.7 %	27.6 %
BE	48.8 %	52.0 %	40.4 %	33.9 %	24.8 %	18.3 %	20.2 %
BG	36.8 %	33.5 %	45.1 %	33.3 %	24.3 %	24.3 %	23.5 %
CY	44.4 %	37.0 %	23.8 %	27.1 %	11.5 %	17.6 %	14.6 %
DE	73.6 %	68.9 %	67.6 %	48.6 %	43.8 %	41.6 %	32.0 %
EE	54.7 %	55.1 %	30.3 %	42.1 %	12.5 %	14.5 %	21.7 %
EL	66.9 %	70.8 %	40.7 %	34.4 %	20.0 %	25.2 %	15.8 %
FI	86.9 %	78.1 %	78.1 %	53.5 %	33.2 %	37.8 %	28.1 %
HR	50.0 %	60.6 %	40.2 %	22.9 %	14.2 %	18.6 %	21.2 %
HU	56.7 %	67.7 %	58.2 %	28.2 %	24.2 %	28.9 %	17.8 %
IT	41.9 %	44.3 %	23.2 %	28.6 %	17.7 %	7.0 %	13.9 %
LT	53.3 %	65.7 %	53.0 %	34.4 %	20.3 %	17.5 %	19.5 %
LU	56.1 %	46.6 %	45.9 %	34.2 %	20.7 %	22.2 %	19.3 %
MT	48.6 %	49.6 %	42.9 %	35.4 %	24.3 %	27.1 %	30.4 %
NL	61.8 %	65.6 %	58.3 %	44.3 %	25.9 %	23.8 %	37.5 %
PL	60.6 %	61.3 %	49.7 %	30.2 %	24.6 %	25.6 %	22.2 %
PT	61.4 %	62.8 %	44.8 %	38.8 %	26.5 %	23.5 %	27.2 %
RO	47.0 %	65.2 %	57.2 %	37.3 %	34.9 %	29.9 %	29.0 %
SE	72.9 %	59.1 %	62.4 %	60.6 %	31.9 %	32.5 %	28.4 %
SI	68.7 %	79.7 %	63.8 %	61.2 %	33.4 %	36.9 %	30.2 %
SK	62.7 %	76.5 %	42.5 %	34.3 %	24.1 %	25.5 %	34.5 %
EU24*	61.9 %	61.0 %	52.3 %	41.0 %	31.7 %	27.4 %	25.4 %

* Media ponderata per i 24 Stati membri dell'UE nella tabella.

Fonte: Community Innovation Survey (CIS 2012), in EUIPO, (nt. 113), 28.

Questa tabella illustra quali meccanismi di protezione utilizzano le imprese in UE per tutelare le proprie innovazioni. I sistemi più impiegati nel periodo 2010-2012 non sono diritti di proprietà intellettuale, bensì, nella maggior parte dei paesi, le forme di tutela sono connesse a vantaggi derivati dalla prima mossa nel mercato e dalla complessità del prodotto commercializzato. I segreti commerciali si posizionano al terzo posto, ad eccezione di Cipro, Estonia e Italia, dove i marchi d'impresa sostituiscono la segretezza nelle prime tre posizioni. Le imprese tedesche risultano le maggiori utilizzatrici di segreti commerciali e brevetti.

B. Tabella esplicativa delle imprese innovative in UE che utilizzano segreti commerciali o brevetti per la protezione delle innovazioni di prodotto o di processo per paese e dimensione, 2010-2012

	Trade Secrets			Patents			Innovating Firms*
	Total	SME	Large	Total	SME	Large	
AT	64.8 %	63.4 %	79.1 %	35.3 %	32.6 %	62.3 %	39.3 %
BE	40.4 %	38.7 %	63.6 %	24.8 %	23.2 %	46.7 %	46.5 %
BG	45.1 %	44.1 %	54.0 %	24.3 %	24.2 %	25.1 %	16.9 %
CY	23.8 %	23.6 %	28.6 %	11.5 %	11.8 %	4.8 %	29.9 %
DE	74.1 %	73.5 %	82.4 %	47.8 %	45.9 %	72.8 %	55.0 %
EE	30.3 %	29.1 %	54.0 %	12.5 %	11.4 %	33.5 %	38.4 %
EL	40.7 %	39.9 %	63.5 %	20.0 %	19.6 %	30.9 %	34.3 %
FI	78.1 %	76.8 %	93.6 %	33.2 %	31.1 %	57.9 %	44.6 %
HR	40.2 %	38.3 %	56.3 %	14.2 %	13.7 %	18.6 %	25.0 %
HU	58.2 %	57.5 %	63.3 %	24.2 %	23.2 %	31.3 %	16.4 %
IE	40.4 %	39.3 %	58.3 %	22.7 %	21.9 %	35.4 %	42.3 %
IT	23.2 %	22.6 %	41.1 %	17.7 %	16.9 %	39.1 %	41.5 %
LT	53.0 %	51.6 %	67.5 %	20.3 %	19.4 %	29.3 %	18.9 %
LU	45.9 %	43.3 %	75.8 %	20.7 %	19.0 %	40.3 %	48.5 %
LV	48.4 %	46.6 %	71.6 %	25.7 %	25.4 %	29.4 %	19.5 %
MT	42.9 %	42.2 %	50.0 %	24.3 %	23.5 %	33.3 %	35.9 %
NL	58.3 %	58.0 %	64.2 %	25.9 %	25.3 %	40.5 %	44.5 %
PL	49.7 %	47.8 %	61.4 %	24.6 %	23.6 %	30.7 %	16.1 %
PT	44.8 %	43.6 %	68.3 %	26.5 %	26.0 %	36.0 %	41.3 %
RO	57.2 %	55.9 %	65.0 %	34.9 %	34.1 %	39.8 %	6.3 %
SE	62.4 %	61.6 %	76.4 %	31.9 %	30.6 %	54.3 %	45.2 %
SI	63.8 %	62.6 %	74.4 %	33.4 %	32.0 %	45.6 %	32.7 %
SK	42.5 %	39.6 %	62.2 %	24.1 %	21.1 %	44.2 %	19.7 %
UK	43.2 %	42.5 %	59.5 %	27.3 %	26.5 %	46.7 %	34.0 %
EU24**	**52.3 %**	**51.2 %**	**69.1 %**	**31.7 %**	**30.4 %**	**52.8 %**	**36.0 %**

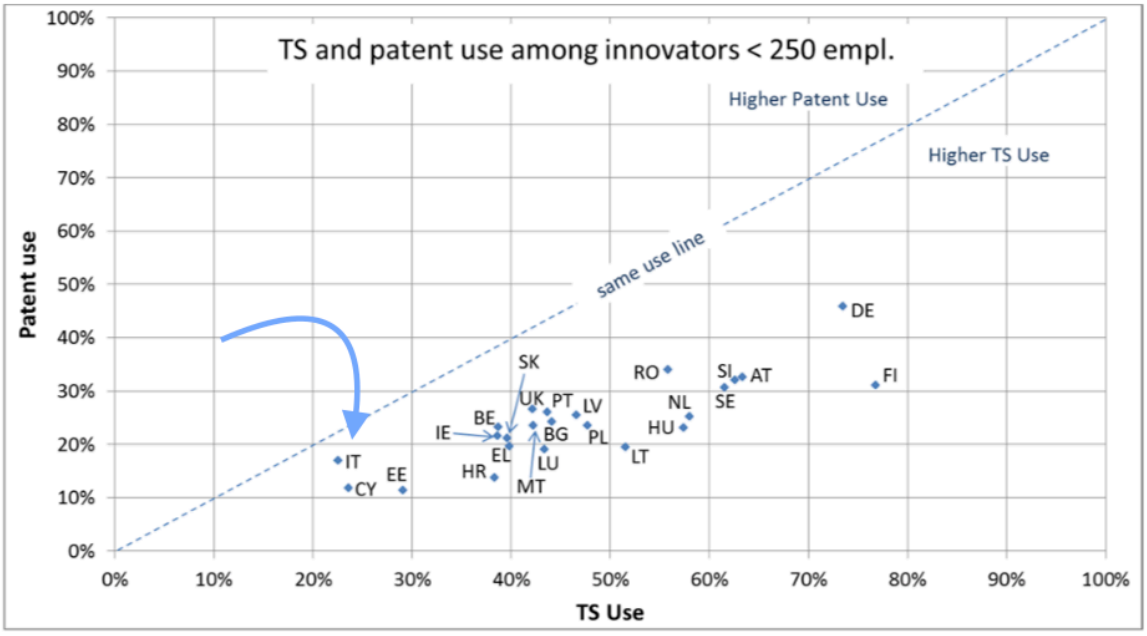
** Media ponderata per i 24 Stati membri dell'UE nella tabella.

Fonte: Community Innovation Survey 2012, in EUIPO, (nt. 113), 30.

La tabella analizza l'utilizzo di segreti commerciali in relazione ai brevetti: i segreti risultano chiaramente superiori in ogni Paese membro della UE, con dati però divergenti tra gli stessi (circa un terzo in più di utilizzo di segreti commerciali in Italia, mentre in Croazia i segreti sono 3 volte superiori). A parte l'Italia, le differenze più piccole tra uso di brevetti e segreti commerciali si riscontrano in Belgio mentre le maggiori differenze, oltre alla Croazia, si evidenziano in Finlandia, Ungheria, Lituania e Paesi Bassi.

C. Grafici sull'utilizzo di segreti commerciali e brevetti tra PMI innovative e grandi imprese per paese, 2010-2012

PMI innovative

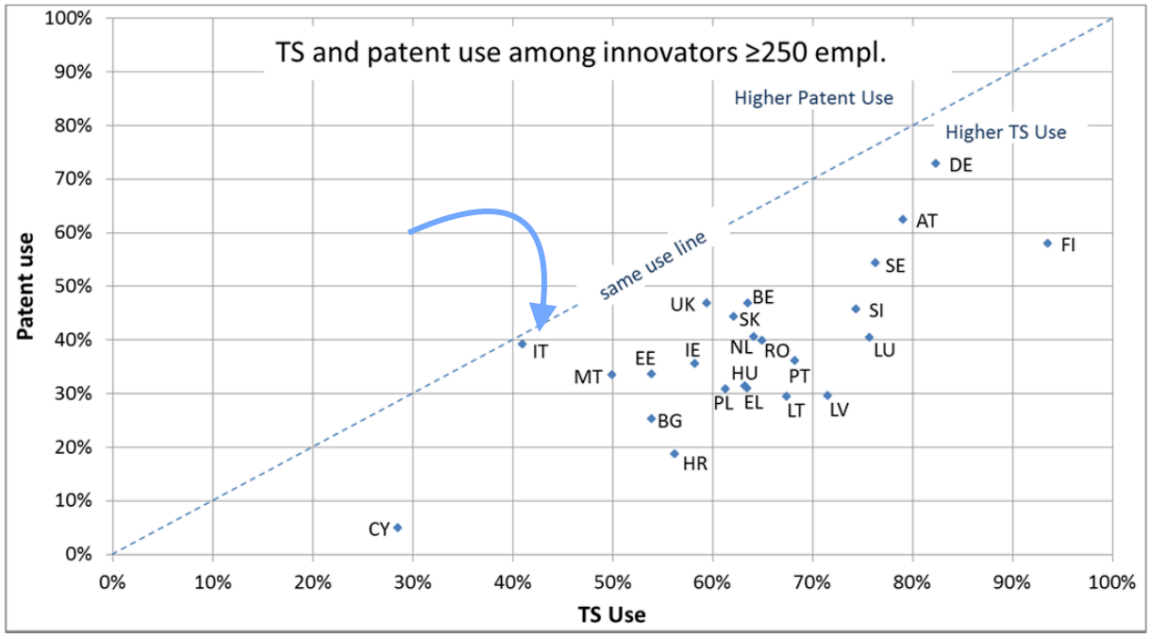


Fonte: Indagine sull'innovazione comunitaria (CIS 2012) in EUIPO, (nt. 113), 32.

Questo grafico, che analizza le PMI, posiziona tutti gli Stati membri al di sotto della linea diagonale, ciò riflette la maggiore prevalenza dell'uso di segreti commerciali rispetto ai brevetti. Le PMI italiane, così come le PMI estoni e cipriote, segnalano i tassi di utilizzo più bassi di entrambi gli strumenti, le PMI italiane sono però più vicine alla linea diagonale, ciò indica una differenza minore nel livello di utilizzo di segreti commerciali e brevetti rispetto ad altri Stati.

All'altro estremo si posizionano le PMI finlandesi innovative, con un uso di segreti commerciali 2,5 volte superiore rispetto a quello di brevetti. Le PMI tedesche segnalano un alto tasso di utilizzo di segreti commerciali (73,5%) ma anche il più alto utilizzo di brevetti (49,5%) tra le PMI nell'UE. Le PMI in Austria, Slovenia, Svezia, Romania, Paesi Bassi e Ungheria hanno tassi elevati di utilizzo di segreti commerciali e brevetti, ma in Ungheria e, in particolare, in Romania, il numero di PMI innovative è basso (come nel caso di Polonia e Bulgaria).

Grandi imprese



Fonte: Indagine sull'innovazione comunitaria (CIS 2012) in EUIPO, (nt. 113), 32.

Questo secondo grafico mostra gli stessi dati di quello precedente, ma per le grandi imprese (con più di 250 dipendenti) nell'UE. L'utilizzo di strumenti di protezione tra grandi imprese varia maggiormente: ad eccezione di Cipro, l'uso di segreti commerciali e brevetti è significativamente più elevato tra le grandi imprese rispetto alle PMI, i paesi tendono infatti a posizionarsi più a destra in questo grafico rispetto al grafico precedente. Le grandi imprese italiane utilizzano invece segreti commerciali e brevetti in proporzioni simili, l'Italia si posiziona infatti quasi sulla diagonale, come nel grafico delle PMI. Anche le grandi imprese tedesche fanno un uso simile sia di segreti commerciali che di brevetti, cosicché la Germania è relativamente vicina alla diagonale ma ad un livello molto più alto rispetto all'Italia. Insieme a Germania, la Finlandia, l'Austria e la Svezia sono i paesi in cui le grandi imprese segnalano il maggior uso di segreti commerciali e brevetti.

BIBLIOGRAFIA E SITOGRAFIA

- ABRIANI N., BOTTINO G., RICOLFI M., *Diritto industriale*, in *Tratt. Cottino*, Cedam, Padova, 2001.

- ACCORDO TRIPS, Marrakech, 1994. URL: https://www.uibm.gov.it/attachments/Accordo_trips.pdf.

- ALMELING D. S., *Seven Reasons Why Trade Secrets Are Increasingly Important*, Berkeley Technological Law Journal, XXVII, 2012.

- ANITEC-ASSINFORM, *Il Digitale in Italia 2020 di Anitec-Assinform, Volume II*, 2020. URL: http://ildigitaleinitalia.it/il-digitale-in-italia-2019/il-digitale-in-italia-2019.kl.

- AQUARO D., *Blockchain, una tutela in cerca d'autore,* IlSole24Ore, 2019. URL: https://www.ilsole24ore.com/art/blockchain-tutela-cerca-d-autore-ACr5GR7.

- AQUARO D., *Marchi, brevetti e opere: così la blockchain difende la proprietà intellettuale*, IlSole24Ore, 2019. URL: https://24plus.ilsole24ore.com/art/marchi-brevetti-e-opere-cosi-blockchain-difende-proprieta-intellettuale-ACaEnZ3.

- AQUARO D., *Smart contract, la clausola si autoesegue*, IlSole24Ore, 2019.

- AREZZO E., *Nuove invenzioni e rapporti tra i diversi requisiti di brevettabilità nella giurisprudenza EPO,* in Il Diritto industriale, Ipsoa, 2016, II.

- AREZZO E., *Protezione del segreto e tutela del software: convergenze, sovrapposizioni, conflitti,* in Il Diritto Industriale, Ipsoa, 2018, II.

- AREZZO E., *Protezione del segreto e tutela del software: convergenze, sovrapposizioni, conflitti,* Filodiritto, 2017. URL: https://www.filodiritto.com/protezione-del-segreto-e-tutela-del-software-convergenze-sovrapposizioni-conflitti

- AREZZO E., *Tutela brevettuale e autoriale dei programmi per elaboratore: profili e critica di una dicotomia normativa*, Giuffrè, Milano, 2012.

- ASCARELLI T., *Teoria della concorrenza e dei beni immateriali*, Giuffrè, Milano, 1960.

- AUTERI P., *Diritto Industriale, proprietà intellettuale e concorrenza*, Torino, Giappichelli Editore, 2020.

- AVI M. S., *Il sistema informativo integrato, Volume I, Analisi aziendali di natura economico-finanziario: il bilancio come strumento di gestione,* Libreria Editrice Cafoscarina, 2019.

- BALBO A., *Segreti commerciali: la Blockchain è una "misura ragionevole" per mantenerli al sicuro?,* Cyberlaws, 2018. URL: https://www.cyberlaws.it/en/2018/blockchain-segreti-commerciali/.

- BANTERLE F., BLEI M., *Alcune novità introdotte dalla direttiva Trade Secrets*, in Il Diritto Industriale, Ipsoa, 2017, IV-V.

- BARBA A., PAGLIANTINI S., *Commentario del Codice Civile, Modulo Delle Persone, Vol. II*, UTET Giuridica, 2019.

- BARBIERO M., *La tutela del know-how e il diritto del lavoro*, Politecnico di Milano, 2015.

- BERENSCHOT B., *Modelli di management. Idee e strumenti,* Prentice Hall, 2005.

- BONA M., CAMUSSO A., OLIVA U.,VERCELLI A, *La tutela del know-how. Diritto industriale, del lavoro, penale e responsabilità civile,* Giuffrè, Milano, 2012.

- BONELLI G., *La tutela dei Big Data quale segreto Industriale,* in Quotidiano Giuridico, UTET Giuridica, 21 marzo 2019.

- BRUSCHI F., *Le applicazioni delle nuove tecnologie: criptovalute, blockchain e smart contract,* in Il Diritto Industriale, Ipsoa, 2020, II.

- CALABRESE B., *Preminenza del brevetto europeo e autonomia del brevetto italiano,* in Giurisprudenza Commerciale, Giuffrè, 2020, III.

- CAMBRIDGE DICTIONARY, voce *assessment*, n.d.. URL: https://dictionary.cambridge.org/it/dizionario/inglese/assessment.

- CAMERA DI COMMERCIO MILANO MONZA BRIANZA LODI, *Segreto commerciale.* URL: https://www.milomb.camcom.it/segreto-industriale.

- CARINCI F., DE LUCA TAMAJO R., TOSI P., TREU T., *Diritto del lavoro 2. Il rapporto di lavoro subordinato*, UTET Giuridica, Torino, 2005.

- CARLINI V., *Wall Street, il dominio degli asset intangibili tocca i 35mila miliardi,* IlSole24Ore, 2020.

- CASELLI E.P., *Codice del diritto d'autore*, UTET Giuridica, Torino, 1943.

- CASSANO G., VACIAGO G., SCORZA G., *diritto dell'internet,* Cedam, 2012.

- CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE, *Guida alla Firma Digitale,* 2009.

- CHESBROUGH H., *The era of open innovation,* 2003.

- CHIABOTTO A., *La protezione dei segreti commerciali: la direttiva UE 2016/943,* in Contratto e impresa/Europa, Cedam, 2016, II.

- CHIEZZI F., in *La tutela del know-how nell'era digitale*, Le Fonti Legal, 2018. URL: https://www.lefonti.legal/la-tutela-del-know-how-nellera-digitale/.

- CICCONE G., GHINI F., *La tutela giudiziale civile dei segreti commerciali anche dopo l'introduzione del d.lgs. n. 63/2018,* in Il Diritto Industriale, Ipsoa, 2019, V.

- CIO, *Come proteggere gli algoritmi dal furto di proprietà intellettuale,* CIO Business Technology Leadership, 2020. URL: https://www.cwi.it/cio/come-proteggere-gli-algoritmi-dal-furto-di-proprieta-intellettuale_42129810.

- CISCO, *Cos'è un firewall?*, URL: https://www.cisco.com/c/it_it/products/security/firewalls/what-is-a-firewall.html.

- COCA-COLA ITALIA, *Dov'è custodita la formula segreta di Coca-Cola?* URL: https://www.coca-colaitalia.it/il-nostro-mondo/curiosita/ricetta-segreta.

- COCCA V., *Responsabilità civile, etica e tutela dei diritti di proprietà intellettuale nei sistemi di intelligenza artificiale,* in Quotidiano Giuridico, UTET Giuridica, 13 aprile 2021.

- CODICE DELLA PROPRIETÀ' INDUSTRIALE a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273. Entrata in vigore del decreto: 19-3-2005 (Ultimo aggiornamento all'atto pubblicato il 19/05/2020).

- COMMISSIONE EUROPEA, *Che cosa sono i dati personali.* URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_it.

- COMMISSIONE EUROPEA, *Digital Economy and Society Index (DESI),* 2020. URL: https://ec.europa.eu/digital-single-market/en/scoreboard/italy.

- COMMISSIONE EUROPEA, *European IPR Helpdesk*, nel *Fact Sheet Trade secrets: An efficient tool for competitiveness,* 2017. URL: https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-Trade-Secrets.pdf.

- COMMISSIONE EUROPEA, *Recovery plan for Europe.* URL: https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

- COMMISSIONE EUROPEA, *The scale and impact of industrial espionage and theft of trade secrets through cyber*, 2018. URL: https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en.

- CONOSCENTI M., VETRO' A., DE MARTIN J.C., *Blockchain for the internet of things: a systematic literature review,* in: 2016 IEEE/ACS 13th International conference of computer systems and applications (AICCSA), New York, IEEE, 2016.

- CONSIGLIA M.M., in *Nuova definizione di valute virtuali: l'orientamento del TAR,* Giustizia civile.com, 2020. URL: https://giustiziacivile.com/banca-finanza-assicurazioni/note/nuova-definizione-di-valute-virtuali-lorientamento-del-tar.

- COSA N. *Come proteggere le proprie invenzioni: brevetto o segreto industriale?* Iusinrete, 2018. URL: https://www.iusinitinere.it/come-proteggere-le-proprie-invenzioni-brevetto-o-segreto-industriale-10432.

- CRESPI A., *La tutela penale del segreto*, Priulla, Palermo, 1952.

- CUPOLO M., *Come tutelare know how e segreti commerciali nell'impresa 4.0,* RiskManagement360, 2020. URL: https://www.riskmanagement360.it/analisti-ed-esperti/come-tutelare-know-how-e-segreti-commerciali-nellimpresa-4-0/.

- CUPOLO M., *Industria 4.0, l'importanza di know how e segreti commerciali,* Industry4business, 2020. URL: https://www.industry4business.it/esperti-e-analisti/industria-4-0-limportanza-di-know-how-e-segreti-commerciali/.

- D'ANNA A., *La formazione del consenso nella blockchain in assenza di autorità centralizzate, il problema dei generali bizantini e prospettive future,* Cyberlaws, 2020. URL: https://www.cyberlaws.it/en/2020/formazione-consenso-blockchain-prospettive-future/.

- DE PALMA S., *La protezione delle informazioni riservate: Non-disclosure Agreement e Confidentiality Clause,* filodiritto.it. URL: https://www.filodiritto.com/la-protezione-delle-informazioni-riservate-non-disclosure-agreement-e-confidentiality-clause.

- DIRETTIVA UE 2016/943 del parlamento Europeo e del Consiglio dell'8 Giugno 2016.

- DI PORTO F., *Big data e concorrenza*, in Concorrenza e mercato, Giuffrè, 2016, XXIII, 5 ss. URL: https://www.researchgate.net/publication/316644215_La_rivoluzione_big_data_Un'introduzione/link/59097aecaca272f658fc01e4/download.

- ENCYCLOPEDIA BRITANNICA, *Middleware computer software,* n.d. URL: https://www.britannica.com/technology/middleware.

- EPO, EUIPO, *Industrie ad alta intensità di diritti di proprietà intellettuale e risultati economici nell'Unione europea. Rapporto di analisi a livello industriale*, 2016, II. URL: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/performance_in_the_European_Union/eperformance_in_the_European_Union_sum-it.pdf.

- EPO, EUIPO, *Industrie ad alta intensità di diritti di proprietà intellettuale e risultati economici nell'Unione europea. Analisi a livello industriale*, 2019, III. URL: https://

euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/IPR-intensive_industries_and_economicin_EU/summary/IP_Contribution_Report_092019_execsum_it.pdf.

- EUIPO, *IPTK basics,* UEB Monaco, 2014. URL: https://euipo.europa.eu/knowledge/course/view.php?id=1738.

- EUIPO, *Protecting innovation through trade secrets and patents: determinants for European Union firms*, 2017. URL: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf.

- EUR-LEX, *OMC: accordi sugli aspetti della proprietà intellettuale attinenti al commercio,* 2017. URL: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=legissum:r11013.

- FALCE V. *Dati e segreti. Dalle incertezze del Regolamento Trade secret ai chiarimenti delle Linee Guida della Commissione UE,* in Il Diritto industriale, Ipsoa, 2018, II.

- FALCE V., *Tecniche di protezione delle informazioni riservate. dagli accordi Trips alla Direttiva sul segreto industriale,* in Il Diritto Industriale, Ipsoa , 2016, III.

- FAZZINI M., *Due Diligence 2019,* Ipsoa, 2019.

- FORTUNATO S., DI NOCCO C., *Corporate governance le fasi e i processi operativi di un'indagine interna o "internal investigation"*, Rivista dei Dottori Commercialisti, Giuffrè, 2018, LXIX.

- FREZZA G., *Blockchain, autenticazione e arte contemporanea,* in Diritto di Famiglia e delle Persone, Giuffrè, 2020, II.

- FROLLA A., *Cybercrimini, 2020 anno nero: sotto attacco sanità, pagamenti cashless e aziende,* LaRepubblica, 2021. URL: https://www.repubblica.it/economia/rapporti/mondo5g/storie/2021/02/24/news/aumento_crimini_informatici_osservatorio_cybersecurity-288979390/.

- GALIMBERTI A., *Maxi condanna per segreti industriali violati,* IlSole24ore, 2019.

- GALLI C., *Il nuovo diritto del know-how e dei segreti commerciali,* UTET Giuridica, 2018.

- GALLI C., *Le nuove frontiere del diritto dei brevetti,* Torino, Giappichelli Editore, 2003.

- GALLI C., *Potenziale perpetuità della tutela del know-how e contrattualizzazione degli impegni di riservatezza,* in Il Diritto Industriale, Ipsoa, 2018, II.

- GALLI C., GAMBINO A., *Codice ipertestuale commentato della proprietà industriale ed intellettuale*, UTET Giuridica, Padova, 2011.

- GARUFI C., *Il brevetto europeo e i segreti commerciali,* La Tribuna, 2018.

- GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA, Anno 159°, Numero 130.

- GERACI A., *Storno di dipendenti: illecito se attuato per utilizzare il know-how del concorrente,* in Il Diritto Industriale, Ipsoa, 2017, IV.

- GHIDINI G., *Profili evolutivi del diritto industriale*, Giuffrè, Milano, 2015.

- GHIDINI G., CAVANI G., *Proprietà intellettuale e concorrenza. Corso di diritto industriale*, Zanichelli, Torino, 2021.

- GIAVAZZI S., *La tutela penale del segreto industriale*, Giuffrè, 2012.

- GITTI G., MAUGERI M., FERRARI C., *Offerte iniziali e scambi di cripto-attività,* in Osservatorio del diritto civile e commerciale, Il Mulino, 2019, I.

- GUALTIERI G., *La tutela penale del know how: la violazione del segreto industriale,* in Il Diritto Industriale, Ipsoa, 2018, II.

- I-COM, Istituto per la Competitività, *Blockchain tra opportunità e sfide,* URL*:* https:// www.i-com.it/wp-content/uploads/2019/11/Blockchain-tra-opportunita-e-sfide.pdf.

- JEDRUSIK A., *Patent protection for software-implemented inventions,* WIPO magazine, 2017. URL: https://www.wipo.int/wipo_magazine/en/2017/01/article_0002.html.

- LANDINI S., *Cyber risk: le polizze assicurative per tutelarsi,* in Quotidiano Giuridico, UTET Giuridica, 6 aprile 2018.

- LIBERTINI M., *Le informazioni commerciali riservate (segreti commerciali) come oggetto di diritti di proprietà industriale,* in Il Diritto industriale, Ipsoa, 2017, VI.

- MACI L., *Che cos'è l'Industria 4.0 e perché è importante saperla affrontare,* NetworkDigital360, 2021. https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare/.

- MAGGIORE M., REGUZZONI M., *Segreti industriali, know-how e blockchain,* Creativitysafe.com, n.d. URL: https://creativitysafe.com/segreti-industriali-know-how-e-blockchain/.

- MAGNA L., *Lupin 4.0, giù le mani dal segreto industriale!*, Industria Italiana, 2019. URL: https://www.industriaitaliana.it/lupin-4-0-giu-le-mani-dal-segreto-industriale/.

- MASSINI M., *Diritto al segreto e diritto alla riservatezza*, privacy.it, 2000. URL: https:// www.privacy.it/archivio/massimi02.html.

- MASTRELIA D., *Gli accordi di trasferimento di tecnologia*, Giappichelli Editore, Torino, 2010.

- MASTRELIA D., *La tutela del know-how, delle informazioni e dei segreti commerciali fra novità normative, teoria e prassi,* in Il Diritto Industriale, Ipsoa, 2019, V.

- MARCHETTI P., UBERTAZZI L.C., *Commentario breve alle leggi sulla proprietà intellettuale e concorrenza,* Cedam, Padova, 2007.

- MARINI P., *Come costruire un sistema di gestione privacy?,* UTET Giuridica, 2019.

- MAUGERI M., *Smart contracts e disciplina dei contratti,* in Osservatorio del diritto civile e commerciale*,* Il Molino*,* 2020, II.

- MINISTERO DEI BENI E DELLE ATTIVITÀ' CULTURALI E DEL TURISMO, *Legge sul diritto d'autore (L. 633/1941).*

- MINISTERO DELLO SVILUPPO ECONOMICO, *Brevetto per modello di utilità,* 2021. URL: https://uibm.mise.gov.it/index.php/it/brevetti/brevetto-per-modello-di-utilita#:~:text=82%20del%20CPI%20stabilisce%20che,nuovi%20modelli%20consistenti%20in%20particolariù.

- MINISTERO DELLO SVILUPPO ECONOMICO, *Disegni e modelli,* 2021. URL: https://uibm.mise.gov.it/index.php/it/disegni-e-modelli.

- MINISTERO DELLO SVILUPPO ECONOMICO, *Procedimento di esame e concessione,* n.d. URL: https://uibm.mise.gov.it/index.php/it/brevetti/deposito-di-una-domanda-di-brevetto/procedimento-di-esame-e-concessione.

- MONDINI G., *Big Data. Processi di big data analytics nelle imprese e nella P.A.: chi è proprietario dei dati?*, in Quotidiano Giuridico, UTET Giuridica, 3 settembre 2019.

- MONTANARINI M., *Contratti di cessione e di uso di know how e concorrenza sleale*, Contratto e Impresa, Cedam, 2007, IV-V.

- MORBIDI C., *I rapporti tra know-how e brevetto,* Brevettinews, 2018. URL: https://brevettinews.it/brevetti/rapporti-tra-know-e-brevetto/.

- MORETTI A., *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679,* in Diritto dell'Informazione e dell'Informatica, Giuffrè, 2018, IV.

- MORRIELLO R., *Blockchain, intelligenza artificiale e internet delle cose in biblioteca,* AIB studi, 2019.

- MOSCON V., *Tecnologie blockchain e gestione digitale del diritto d'autore e connessi,* in Il Diritto Industriale, Ipsoa, 2020, II.

- NOCERA C., *Il nuovo regolamento privacy,* Maggioli Editore, Rimini, 2018.

- NYUMBAYIRE, *Il Consenso di Nakamoto*, Interlogica, 2017.

- OLIVI G., *Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti,* in Il Diritto Industriale, Ipsoa, 2020, II.

- OMODEI R. E*, La tutela penale del segreto commerciale in Italia. Fra esigenze di adeguamento e possibilità di razionalizzazione,* Diritto Penale Contemporaneo, Rivista Trimestrale, 2019 *URL:* https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_omodei.pdf.

- OTTOLIA A., *Il D.lgs. n. 63/18 di attuazione della dir. 2016/943/UE sulla protezione dei segreti commerciali fra tutela e bilanciamenti*, Le Nuove Leggi Civili Commentate, Cedam, 2019.

- PANATTONI B., *Compliance, cybersecurity e sicurezza dei dati personali,* Ipsoa, 2020.
- PANZIRONI V., *Per i nuovi dati arriva la sfida di nuove regole*, IlSole24ore, 2016.
- QUAGLI A., *Bilancio e principi contabili 2020,* Ipsoa, 2020.
- QUARANTA A., *Professioni verdi: guida ai green jobs,* Wolters-Kluwer, 2021.
- QUARANTA A, *Sistemi di Gestione Ambientale,* in Ambiente & sviluppo, Ipsoa, 2020, V.
- SALVATORE E., *Know how - rivalutazione e patrimonializzazione del segreto commerciale - Un valore che non può andare perso,* Youcanprint, Lecce, 2020.
- SALZA E., *Opportunità della digitalizzazione e rischi di cybercrime,* IlSole24Ore, 2021.
- SANDRI S., *La nuova disciplina della proprietà industriale dopo i GATT-TRIP's*, Cedam, Padova, 1996.
- SANTOSUOSSO D.U., *Commentario del codice civile, delle società dell'azienda della concorrenza, art. 2575-2642,* Utet Giuridica, 2014.
- SARZANA F., *Copyright: il valore della blockchain come strumento di prova nel processo civile,* IlSole24Ore, 2018. URL: https://fulviosarzana.nova100.ilsole24ore.com/2018/11/24/copyright-il-valore-della-blockchain-come-strumento-di-prova-nel-processo-civile/.
- SARZANA F., NICOTRA M., *Diritto della Blockchain, Intelligenza Artificiale e IoT,*, Ipsoa, Milano, 2018.
- SENA G., *Invenzioni brevettabili e intelligenza artificiale*, in Diritto Industriale, Giuffrè, 2020, II.

- SERAFINI S., *Luci ed ombre della nuova disciplina sul segreto commerciale,* in Il Corriere giuridico, Ipsoa, 2018, XI.

- SHILLING M. A., F. IZZO, *Gestione dell'innovazione*, McGraw-Hill, 2017.

- SPEDICATO G., *Creatività artificiale, mercato e proprietà intellettuale*, in Diritto Industriale, Giuffrè, 2019, IV.

- STELLA M., C*orte di cassazione: decisioni di interesse procecessual-internazionalistico*, Ipsoa, 2016.

- STOLTERMAN E., CROON FORS A., *Information Technology and the Good Life, in Information Systems Research: Relevant Theory and Informed Practice*, 2004.

- RAMACIOTTI L., *Know how,* Treccani Dizionario di Economia e Finanza, 2012. URL: https://www.treccani.it/enciclopedia/know-how_%28Dizionario-di-Economia-e-Finanza%29/.

- RESTA G., *Diritti esclusivi e nuovi beni immateriali,* UTET Giuridica, 2011.

- RICOLFI M., *Motori di ricerca, link sponsorizzati e diritto dei marchi: il caso Google di fronte alla corte di giustizia,* Informatica giuridica e diritto dell'informatica, UTET Giuridica, 2014.

- ROTONDI F., *Diritto del lavoro e delle relazioni industriali 2017*, Ipsoa, 2016.

- TERZI G., *Una nuova stagione per la cybersicurezza*, IlSole24Ore, 2017.

- TOSI E., *La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR),* Studium Iuris, 2020.

- TRECCANI, voce *Copyright,* n.d. URL: https://www.treccani.it/enciclopedia/copyright/#:~:text=(termine%20inglese%2C%20che%20significa%20%22,negli%20Stati%20Uniti%20d%E2%80%99America.

- TRECCANI, voce *Reverse engineering,* 2008. URL: https://www.treccani.it/vocabolario/reverse-engineering_%28Neologismi%29/#:~:text=Il%20%C2%ABreverse%20engineering%C2%BB%20(letteralmente,e%20replicarle%20a%20buon%20mercato.

- TRECCANI, voce *Software,* n.d., URL: https://www.treccani.it/vocabolario/software/.

- TRECCANI, Dizionario di economia e Finanza, voce *Uruguay Round*, 2012. URL: https://www.treccani.it/enciclopedia/uruguay-round_%28Dizionario-di-Economia-e-Finanza%29/.

- TREVISI C., *La regolamentazione in materia di Intelligenza Artificiale, robot, automazione: a che punto siamo*, Medialaws, 2018.

- VANZETTI A., DI CATALDO V., *Manuale di Diritto Industriale,* Giuffrè, Milano, 2018.

- VITALI D., *Covid-19 e sfida digitalizzazione, ultima chiamata per l'Italia*, IlSole24Ore, 2020. URL: https://www.ilsole24ore.com/art/covid-19-e-sfida-digitalizzazione-ultima-chiamata-l-italia-ADauBwg.

- VENIER O. *Intelligenza Artificiale, Blockchain e mondo IoT: l'esperienza degli operatori,* in Il Diritto industriale, Ipsoa, 2020, II.

- VERBAUWHEDE KOGLIN L., *"In Confidence". Putting in Place a Trade Secret Protection Program in an SME,* WIPO*,* 2014. URL: https://www.wipo.int/edocs/mdocs/sme/en/wipo_smes_amm_14/wipo_smes_amm_14_t5.pdf.

- VESSIA F., *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, Giuffrè, Milano, 2019.

- ZAMA A., CALVELLO S., *Segreto - Tribunale di Bologna: concorrenza sleale per sottrazione di segreti e storno di dipendenti,* Filodiritto, 2017.

- ZANONI P., CASATI L. *La durata dei patti di riservatezza: dal termine di un obbligo di non facere al termine del diritto d'uso del bene informazione*, in i Contratti, Ipsoa, 2018, V.