

10 settembre 2018

Giancarlo Buccarella

TUTELA E LIMITI DEI SEGRETI COMMERCIALI

INDICE

1. Modello concorrenziale <i>vs</i> modello proprietario.....	- 1 -
2. Direttiva <i>Trade Secrets</i> : le ragioni della tutela rafforzata. La responsabilità oggettiva del terzo	- 4 -
3. <i>Know-how</i> e segreto commerciale.....	- 9 -
4. Il segreto commerciale nel c.p.i.: il carattere aziendale dell'informazione e la tutela del <i>know-how</i> accademico.....	- 10 -
5. Segretezza e <i>reverse engineering</i>	- 13 -
6. Il valore economico del segreto	- 15 -
7. L'adozione di adeguate misure di protezione.....	- 16 -
8. Limiti alla tutela del segreto commerciale	- 19 -
9. L'eccezione da whistleblowing.....	- 23 -
10. Qualche riflessione finale.....	- 26 -

ABSTRACT

Lo scritto offre una lettura delle norme del codice di proprietà industriale in tema di tutela dei segreti commerciali alla luce ed in conformità ai dettami della Direttiva (UE) 2016/943. Ne deriva (i) un ampliamento dell'ambito oggettivo di tutela, esteso al know-how accademico; (ii) una rilettura in senso pro-concorrenziale del c.d. reverse engineering; (iii) il recupero delle cause di liceità ed eccezioni previste nella direttiva comunitaria. La tutela rafforzata del segreto non è assoluta e incontra alcuni limiti: essa si arresta (o deve essere bilanciata) di fronte ad altri interessi legittimi in conflitto. Infine, è ridimensionata l'idea che il segreto commerciale rafforzato abbia un effetto competitivo sul brevetto, e si avanza la tesi che i divieti di brevettazione, posti per contrarietà all'ordine pubblico o al buon costume, costituiscano un limite alla tutela in regime di segretezza delle informazioni tecniche.

1. Modello concorrenziale vs modello proprietario

Nel nostro ordinamento la tutela (civile) contro l'illecita appropriazione di quello che tradizionalmente è chiamato il segreto industriale era affidata alla disciplina della concorrenza sleale¹, secondo il paradigma ed in forza della clausola di chiusura dell'art. 2598, n. 3 c.c.; nel 1996, con il recepimento dell'Accordo TRIPs e l'introduzione nella legge sui brevetti dell'art. 6 bis, si ha tipicizzazione (parziale) della fattispecie²; successivamente, con l'emanazione del codice della proprietà industriale nel 2005, l'informazione aziendale riservata assurge ad oggetto di diritto autonomo e non titolato di proprietà industriale³

¹ A. FRIGNANI, *Segreti d'Impresa* (voce), in *Dig. it. disc. priv.*, Sez. Comm., XIII, Torino, 1996, 337, ove anche ampie indicazioni bibliografiche.

² A. BLANDINI, *Know-how* (voce), in *Enc. dir.*, Aggiornamento, I, Milano, 1997, 741; P. AUTERI, *Sub art. 14*, in *Commentario al d.lgs. 19 marzo 1996, n. 198*, in *Nuove leggi civili*, 1998, 131; G. DALLE VEDOVE, *La violazione del segreto industriale tra vecchio e nuovo diritto*, in *Riv. dir. ind.*, 1998, 245; N. ABRIANI, G. COTTINO, *I brevetti per invenzione e per modello*, in *Trattato di diritto commerciale*, diretto da G. Cottino, II, Padova, 2001, 247; A. FRIGNANI, *op.cit.*, 350.

Contra, ma sul piuttosto debole argomento topografico, A. CAMUSSO, *Know-how e segreto nell'evoluzione delle fonti*, in M. Bona, A. Camusso, U. Oliva, A. Vercelli (a cura di), *La tutela del Know-how*, Milano, 2002, per il quale se l'art 6 bis l.inv. (abr.) fosse «una specificazione degli atti contrari alla correttezza professionale ex art. 2598, n. 3 c.c., sarebbe stato certo sufficiente modificare quest'ultima norma, piuttosto che introdurre invece nelle leggi brevetti una disposizione ad hoc, delimitata dall'inciso «fatte salve le disposizioni in materia di concorrenza sleale» (7).

Per la residua tutela concorrenziale delle informazioni riservate ma difettevoli dei crismi della legge brevetti, ed oggi del codice p.i., D. SBARISCA, *La tutela concorrenziale delle informazioni «meno riservate»*, in *Dir. ind.*, 2018, 127.

³ G. FLORIDIA G., *Il riassetto della proprietà industriale*, Milano, 2006, e dello stesso A., *Le creazioni protette*, in AA.VV., *Diritto industriale. Proprietà intellettuale e concorrenza*, 5a ed., Torino, 2016, 210. Chiaro del resto il disposto dell'art. 1 c.p.i. per il quale l'espressione proprietà industriale comprende «informazioni aziendali riservate», locuzione sostituita con «segreti commerciali», in attuazione della Direttiva (UE) 2016/943. Questa impostazione del codice è

(art. 1 c.p.i), riservandosi alla sua disciplina due precise disposizioni, l'art. 98 e l'art. 99, quest'ultima, oggetto di successiva modifica ad opera del decreto correttivo, d.lgs. n. 131/2010; infine, in attuazione della Direttiva (UE) 2016/943 dell'8 giugno 2016 (nell'uso contratto, Direttiva *Trade Secrets*⁴), il d.lgs. 11 maggio 2018, n. 63, interviene sul Codice p.i., con disposizioni sostanziali (a modifica degli artt. 1, 2 comma 4, 98, 99) e processuali (a modifica degli artt. 124, 126, 132, e inserendo l'art. 121 *ter*) e sul codice penale⁵ (a modifica degli artt. 388 e 623 c.p.).

Dunque, fino all'emanazione del Codice p.i., contro l'appropriazione illecita dei segreti industriali - salva la tutela contrattuale per violazione di patti di segretezza, per la quale nulla è innovato - si poteva reagire invocando una tutela non assoluta (estesa cioè contro i terzi in buona fede), bensì relativa (contro chi abbia illecitamente conosciuto il segreto), di natura extracontrattuale e condizionata alla ricorrenza di modalità di sottrazione sleali. Questo modello di tutela concorrenziale era generalmente adottato da altri Paesi, nonché dal diritto internazionale, giusto l'art. 39 dell'accordo TRIPS⁶. Ne discendevano, a quanto comunemente ritenuto, alcuni esiti ricostruttivi della fattispecie: il segreto aziendale non era tutelato in sé, né, perciò, vi era un corrispondente diritto al

stata per lo più oggetto di critiche: G. SENA, *Efficienza e inefficienza della macchina normativa (note sui c.d. diritti non titolati)*, in *Riv. dir. ind.*, 2012, I, 83; A. VANZETTI, *La tutela "corretta" delle informazioni segrete*, in *Riv. dir. ind.*, 2011, 96; G. GHIDINI, *La tutela del segreto: critica di una "riforma"*, in *Dir. ind.*, 2008, 167. Condivide l'impianto codicistico, M. LIBERTINI, *Le informazioni aziendali segrete come oggetto di diritti di proprietà industriale*, in *Riv. it. sc. giur.*, 2011, 137.

⁴ F. BANTERLE, M. BLE, *Alcune novità introdotte dalla direttiva Trade Secrets*, in *Riv. dir. ind.*, 2017, 202. Per un esame del processo di adozione della Direttiva, V. FALCE, *Tecniche di protezione delle informazioni riservate. Dagli accordi TRIPS alla Direttiva sul segreto Industriale*, in *Riv. dir. ind.*, 2016, 129; G. CHIAPPETTA, *La proposta di direttiva e le linee di evoluzione della disciplina del Know-how rectius delle informazioni aziendali riservate*, in *Dir. ind.*, 2016, 171.

⁵ La pena edittale per il delitto di rivelazione di segreti commerciali, punibile a querela, è la reclusione fino a tre anni (art. 623 c.p.); senza considerare i vari e indulgenti istituti processuali e di diritto materiale che incidono sulla determinazione della pena, la norma penale è decisamente assai poco deterrente in raffronto ai 10 anni di pena detentiva e comminazione di multa fino a 5 milioni di dollari previste dall'*Economic Espionage Act* del 1996 (18 U.S.C. § 1832(a)); nel caso di spionaggio industriale straniero la pena detentiva è fino 15 anni e la multa, se vi è responsabilità di *organization*, è fino a 15 milioni di dollari o tre volte il valore dei *trade secrets* violati, cfr. A. WAKS, *Where the Trade Secret Sits: How the Economic Espionage Act is inflaming Tensions in the Employment Relationship, and How Smart Employers and Employees are responding* 3 N.Y.U. J. of Intell. Prop. & Ent. Law 395 (2014).

⁶ Che così fosse, non v'è dubbio, per via del riferimento generale dell'art. 39 all'art. 10 *bis* della Convenzione di Parigi. Cfr. A. VANZETTI, *La tutela "corretta"*, cit., 99, il quale osserva che la tutela delle informazioni segrete rivelate a terzi oppure acquisite o utilizzate da parte di terzi «in un modo contrario a leali pratiche commerciali» (art. 39 n. 2), riprende la terminologia tipica della disciplina della concorrenza sleale.

segreto, e neppure era accettata una sua oggettivizzazione come bene giuridico immateriale⁷.

L'accolta concezione c.d. proprietaria⁸ del segreto industriale trovò la netta critica di una parte ed autorevole dottrina (Ghidini), per le profonde distonie sistematiche intraviste e gli affermati effetti anticoncorrenziali del segreto, con esiti esiziali: (i) incoraggiamento a privilegiare l'uso dei trovati in regime di segretezza, in danno del regime brevettuale e con ostacolo degli effetti benefici, per la concorrenza e l'innovazione, collegati allo scambio tra attribuzione dell'esclusiva di durata certa e limitata ed integrale *disclosure* dell'innovazione⁹; (ii) "privatizzazione" dei risultati della ricerca che la normativa brevettuale, diversamente, esclude da privata¹⁰. E tutto ciò, si faceva notare, a protezione di interessi «scarsamente meritevoli», di una industria che "non ce la fa" ad innovare seriamente¹¹.

⁷ Il concetto è espresso mirabilmente dall'Ascarelli (in *Teoria della concorrenza e dei beni immateriali*, Milano, 1960): il segreto non è «tutelato come tale e non v'è corrispondentemente un diritto al segreto; [esso] è indirettamente tutelato data la protezione che gli deriva dalla preclusione (perché illeciti) di mezzi che dovrebbero servire a carpirlo ed è in quanto esso sia stato illecitamente o fiduciariamente conosciuto che sussiste un divieto di divulgazione e utilizzazione. Divieto che però sussiste nei confronti di chi lo abbia così illecitamente o fiduciariamente conosciuto o in genere quando e in quanto dettato e non già come conseguenza di un generale divieto assoluto al segreto»; deve, aggiunge l'illustre Maestro, essere perciò esclusa «la possibilità di considerare il "segreto" come un bene oggetto di diritto assoluto, come pur a volte tende a fare un'autorevole dottrina attraverso quell'estensione del concetto di bene immateriale che abbiamo già esaminato e criticato in tema di avviamento e di concorrenza (...)» (285).

⁸ Nota il Libertini (*Le informazioni commerciali riservate (segreti commerciali) come oggetto di diritti di proprietà industriale*, in *Dir. ind.*, 2017, 569) che nell'esperienza statunitense l'idea di un «*Property right*» sui segreti aziendali si è originariamente sviluppata nel quadro generale della *Common law*, è stata quindi affermata con l'*Union Trade Secrets Act* del 1979 e di recente dalla legge federale *Defend Trade Secrets Act* del 2016. V., anche, R. G. BONE, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 Calif. L. Rev. 252-253 (1998), che riporta l'*opinion* del giudice Gray nel caso *Peabody v. Norfolk* (98 Mass. 452 (1868)), ove per prima si avanzò l'idea del *property right* («*If a man establishes a business and makes it valuable by his skill and attention, the good will of that business is recognized by the law as property*»). Francis Peabody aveva inventato un nuovo processo e una macchina per la produzione di tela di juta. Impiantò una fabbrica ed assunse Norfolk come macchinista, impegnandolo, con un patto di non concorrenza, a non usare o divulgare il processo segreto. Qualche tempo dopo, Norfolk si unì a James Cook ed altri uomini d'affari, per costruire un impianto concorrente, usando i macchinari e il processo di Peabody. Nella causa che ne seguì, la Corte Suprema del Massachusetts accolse le richieste di tutela di Peabody.

⁹ Cfr. R. G. BONE, *A New Look at Trade Secret Law*, cit., 266 (1998): «If an inventor chooses trade secret instead of patent, others will be denied ready access to the information, access that would exist under patent law». Questa funzione è tuttavia oggetto di critica: Lemley osserva che molte imprese non leggono i brevetti prima di sviluppare nuovi prodotti (M. A. LEMLEY, *The Surprising Virtues of Treating Trade Secrets as IP Rights* 61 Stan. L. Rev. 311, 333 nt. 89 (2008)).

¹⁰ Così, il Ghidini (*La tutela del segreto*, cit., 168-169) il quale si rammarica di non essersi opposto con sufficiente forza all'interno della commissione ministeriale che predispose la bozza del Codice.

¹¹ *Ibidem*.

Soprattutto, ed è questo un punto di maggior critica, la piena adesione alla concezione proprietaria, postula (postulerebbe) l'assolutezza del diritto proprietario del segreto di fronte al quale soggiace (soggiacerebbe) il terzo in buona fede, e cioè quel terzo che si sia sì oggettivamente avvantaggiato di un segreto altrui, ma in perfetta buona fede, ignorata l'illecita altrui sottrazione, ed estraneo all'illecita altrui condotta: è il caso del nuovo datore di lavoro di un ex dipendente infedele che presenti come frutto di sua propria ideazione un'innovazione sviluppata, e comunque appresa, con vincolo di segreto, nell'azienda dell'ex datore di lavoro. La critica spinge fino al punto di svuotare la riforma di questa naturale e logica conseguenza. Lo si fa, con una *ermeneutica difensiva*, per mutuare le parole del Ghidini, che, seppur con qualche cautela premessa, ragionando per argomenti di teoria generale, afferma che al terzo in buona fede giovi la regola del possesso vale titolo (art. 1153 c.c.); immunizzata, in questo modo, la pretesa risarcitoria, inibitoria e reale del detentore del segreto¹².

Il d.lgs. 131 del 13 agosto 2010 mette nuova mano all'istituto. A modifica dell'articolo 99 del Codice, è inserito l'inciso «in modo abusivo» riferito alla condotta che deve caratterizzare l'appropriazione del segreto; la relazione illustrativa spiega la modifica in questi termini: la nuova disposizione «sostituisce il comma 1 dell'articolo 99 del Codice, riformando il testo per renderlo conforme all'art. 39 dell'accordo Trips», e cioè con richiamo al modello concorrenziale del segreto¹³, tanto da essersi affermato (da una parte della dottrina) un arretramento dei «paletti» della tutela, non più estesa contro il terzo in buona fede¹⁴.

2. Direttiva *Trade Secrets*: le ragioni della tutela rafforzata. La responsabilità oggettiva del terzo

¹² Riguardo l'acquisizione di informazioni segrete da parte di terzi in buona fede, G. GHIDINI, *ivi*, osserva che il terzo, in questa ipotesi, potrebbe invocare la regola generale prevista all'art. 1153 c.c.. In particolare, avendo il legislatore del Codice p.i. costruito il segreto come oggetto di proprietà e configurandosi quindi lo stesso segreto, in quanto bene immateriale, come un bene mobile non registrato, dovrebbe valere, nel caso di «acquisto» dell'informazione riservata da parte di un terzo in buona fede, la regola «possesso vale titolo» prevista appunto all'art. 1153 c.c. Conseguentemente, applicandosi questa norma, il terzo potrebbe utilizzare lecitamente le informazioni segrete.

¹³ Nega il ritorno all'originaria impostazione fondata sulla concorrenza sleale, A. OTTOLIA, *Commento all'art. 99 C.P.I.*, in *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, a cura di P. Marchetti, L. Ubertaini, Padova, 2012, 426. *Contra*, A. FRIGNANI, *Le nuove norme in tema di proprietà industriale*, in *Dir. ind.*, 2011, 10.

¹⁴ M. PASTORE, *La tutela del segreto industriale nel sistema dei diritti di privativa*, in *Diritti esclusivi e nuovi beni immateriali*, a cura di G. Resta, Milano, 2011, 299.

Se in passato gli episodi di spionaggio industriale erano da imputare a “talpe interne”¹⁵ o comunque a chi poteva avere un accesso fisico alla struttura, oggi le imprese vedono moltiplicare la loro vulnerabilità, a causa della digitalizzazione delle informazioni¹⁶ e per via delle nuove e diffuse forme interorganizzative presenti¹⁷: sono numerosi gli attacchi che riguardano piccole realtà e grandi multinazionali, dove i recenti casi di Uber, Yahoo, Equifax, sono solo alcune tra le vicende note¹⁸.

Il diffondersi dei servizi di *cloudcomputing*, ossia la possibilità (o forse meglio la necessità organizzativa) di esternalizzare la gestione dei dati, cambia le regole del gioco, «aprendo la porta agli hacker». E la sottrazione dei dati riservati nonché il furto di proprietà intellettuale per essere rivenduta al mercato nero assume dimensioni enormi¹⁹, creando preoccupazione per la tenuta della competitività di interi Paesi²⁰, con sospetti di spionaggio governativo²¹.

¹⁵ Un caso noto di spionaggio industriale nell’ambito nelle competizioni sportive è quello della McLaren in danno della Ferrari: il capo meccanico della scuderia Ferrari, Nigel Stepney, indispettito per una promozione non ricevuta, passò i progetti della monoposto F2007 all’amico capo progettista di McLaren, Mike Coughlan. La vicenda portò alla condanna della McLaren da parte della FIA, con una penalizzazione di punti del mondiale costruttori e una multa di 100 milioni di dollari, cfr. G. RUSCONI, *La sentenza FIA sulla spy story: via i punti alla McLaren, nessuna penalità ai piloti*, *IlSole24Ore*, 13 settembre 2007.

¹⁶ La rivoluzione digitale impone adeguate politiche di *private enforcement* a tutela dei segreti, M. LIBERTINI, *Le informazioni commerciali riservate*, cit., 571.

¹⁷ L’attività innovativa è sempre più radicata all’interno di reti interpersonali e interorganizzative che implicano relazioni di prossimità, cfr. F. RAMELLA, *Sociologia dell’innovazione economica*, Bologna, 2013, 184. Diversi approcci allo studio dell’innovazione pongono attenzione alla distribuzione e al radicamento spaziale dei processi innovativi, v. P. KRUGMAN, *What’s New about the New Economic Geography?* 14 *Oxford Rev. Econ. Policy* 7-17 (1998).

¹⁸ L. TREMOLADA, *L’outsourcing più della «nuvola» ha spalancato le porte agli hacker*, in *IlSole24Ore*, 23 novembre 2017.

¹⁹ Secondo il rapporto (febbraio 2018) «Economic Impact of Cybercrime - No Slowing Down» (reperibile su <https://www.csis.org/analysis/economic-impact-cybercrime>), la criminalità informatica costa alle imprese quasi 600 miliardi di dollari, pari allo 0,8% del Pil globale, in aumento rispetto allo studio precedente che nel 2014 ha stimato le perdite globali in circa 445 miliardi di dollari.

²⁰ S. BIAGIO, *Moda Italiana nel mirino dei cyber-attacchi*, in *IlSole24ore*, 10 aprile 2017, ove il dato di una indagine dei settori più colpiti dell’economia italiana: 38% fashion, 22% banche, 18% automotive, 12% food&beverage e 10% chimico-farmaceutico.

²¹ Cfr. E. NETTI, *Finanza, tech e industria nel mirino degli hacker*, in *IlSole24Ore*, 30 aprile 2018, che ricorda come in Cina opererebbe la temuta Unità 61398, divisione dell’esercito popolare, accusata più volte di spionaggio industriale ai danni di imprese del mondo occidentale.

V., anche, R. WILKE, *Two Silicon Valley Cases Raise Fears of Chinese Espionage*, in *Wall Street Journal*, 15 gennaio 2003, il quale dà notizia dell’offensiva cinese ai danni di 34 aziende hi-tech della Silicon Valley. Per ulteriori indicazioni sullo spionaggio governativo, D. S. TUCKER, *The Federal Government’s War On Economic Espionage* 18 *U. Pa. J. Int’l Econ. l.* 1109 (1997), H. NASHARI, *Economic Espionage and Industrial Spying*, Cambridge University Press, 2004.

La quarta rivoluzione industriale (c.d. *Internet of Things*) e la rivoluzione digitale nel momento in cui rendono fruibile in modo a-territoriale e pervicace enormi quantità d'informazioni²², con un effetto, per dirla con un'espressione della Falce, *disruptive*²³, impongono un'insopprimibile domanda di maggior tutela del patrimonio di conoscenze del mondo produttivo.

Queste preoccupazioni ed esigenze, unite ad altre, trasfuse nei considerando della Direttiva²⁴, hanno indotto il legislatore europeo a percorrere la strada di una armonizzazione delle normative degli Stati membri che ha portato, nell'ottica di una effettiva Unione dell'Innovazione, e a partire, da un iniziale studio promosso dalla Commissione Europea²⁵ nel 2011, all'adozione della Direttiva (UE) 2016/943 dell'8 giugno 2016 «Sulla protezione del know how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti».

²² D.E. BAMBAUER, *Secrecy is Dead - Long Live Trade Secrets* 93 *Denver University Law Rev.* 833 (2016) che osserva come Daniel Ellsberg ha dovuto fotocopiare lentamente i documenti del Pentagono, mentre Wikileaks, Bradley Manning e Edward Snowden hanno rivelato più informazioni, per ordine di grandezza e con maggiore facilità e in minor tempo.

²³ V. FALCE, *Tecniche di protezione delle informazioni*, cit., 129.

²⁴ Il fatto (i) che le imprese investono nell'acquisizione e nello sviluppo dell'applicazione di know-how e di informazioni segrete e che i segreti commerciali svolgono un ruolo importante nella proteggere lo scambio di conoscenze delle imprese incluse in particolare le PMI (Considerando 2 e in dottrina, J. DE WERRA, *Patents and Trade Secrets in the Internet Age*, in *Zeitschrift für Schweizerisches Recht*, 2015, 166. Il livello di protezione dei segreti commerciali, varia da stato a stato, e questo influenza il *firm-level decision-making*, cfr. M. SCHULTZ, D. LIPPOLDT, *Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper, OECD Trade Policy Papers*, Paris, 2014, n. 162, 25, i quali presentano un indicatore per valutare la severità della protezione esistente: il *Trade Secrets Protection Index*; e sulla base di esso un punteggio dei diversi paesi presi ad esame); (ii) che pur essendo una delle forme di protezione delle creazioni intellettuali delle conoscenze innovative più comunemente usate, sono nel contempo la forma di protezione meno tutelata nell'attuale quadro giuridico dell'Unione (Considerando 3); (iii) che, nonostante l'Accordo TRIPS, tra le legislazioni degli Stati membri sussistono importanti differenze per quanto riguarda la protezione dei segreti commerciali, a partire dalla circostanza che non vi è una definizione unitaria (Considerando 5 e 6); (iv) che le differenze esistenti nella protezione giuridica provocano una frammentazione del mercato interno scoraggiando le imprese dall'intraprendere attività economiche transfrontaliere innovative (Considerando 8). A tal proposito, la letteratura economica ha dimostrato che in assenza di adeguata protezione, la particolare natura di queste conoscenze riservate ne ostacola una loro pur limitata circolazione negoziale: fin quando non ne sia messo al corrente chi voglia pagare per farsele rivelare non si può stimare il loro valore; mentre dopo averle conosciute, in assenza di adeguata tutela, il terzo non ha più interesse a pagare un corrispettivo di acquisto o di licenza, cfr.: G. J. STIGLER, *The Economics of Information* 69 *Journal of Political Economy* 213 (1961), K. J. ARROW, *Economic Welfare and the Allocation of Resources for Invention*, in *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton University Press, 1962 e reperibile su <http://www.nber.org/chapters/c2144.pdf>.

²⁵ Reperibile su http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.htm#contentSec6.

La Direttiva *Trade Secrets*, fondata sull'art. 114 TFUE, e recentemente attuata dal nostro legislatore: (i) armonizza la definizione di segreto commerciale; (ii) identifica le forme più rilevanti di acquisizione illecita; (iii) stabilisce i limiti della protezione con la previsione di cause di liceità e di eccezioni; (iv) detta norme processuali su misure, procedure e strumenti di tutela, anche di carattere provvisorio e cautelare; (v) estende la tutela nei confronti del terzo, che abbia violato inconsapevolmente il segreto, colpendo sia la condotta di utilizzo del segreto, che quella di (produzione e) commercializzazione di merci in violazione del segreto (art. 4, parr 4, 5 e Considerando 6)).

È previsto, a favore del terzo in buona fede, un meccanismo rimediabile più indulgente e cioè il pagamento di un indennizzo su base di calcolo *royalty*, anziché l'adozione delle misure ordinariamente comminabili in caso di illecito (art. 12 Direttiva) - cessazione o divieto di utilizzo del segreto, divieto di produzione, offerta, commercializzazione e utilizzazione di merci, importazione, esportazione, richiamo dal mercato delle merci, distruzione delle merci, distruzione della totalità o di una parte dei documenti, oggetti ecc. che contengono il segreto commerciale - a condizione che:

(i) il terzo sia «a conoscenza o secondo le circostanze, avrebbe dovuto essere a conoscenza» del fatto che il segreto commerciale sia stato sottratto direttamente o indirettamente in modo illecito. Questa ipotesi ricorre nel solo caso in cui il soggetto «abbia originariamente acquisito un segreto commerciale in buona fede, ma abbia appreso solo in un momento successivo, ad esempio all'atto della notifica da parte del detentore originario del segreto commerciale, che la sua conoscenza del segreto in questione proveniva da fonti che stavano utilizzando o divulgando il segreto in questione in modo illecito» (Considerando n. 29 Direttiva)²⁶;

(ii) se vi è danno sproporzionato al soggetto interessato;

(iii) se l'indennizzo appare alla parte lesa ragionevolmente soddisfacente.

Il legislatore italiano ha attuato le prescrizioni della Direttiva (artt. 99, comma 1 *bis*, 1 *ter*, e art. 124, comma 6 *ter*, c.p.i), con l'unica esclusione dell'ultima delle condizioni poc'anzi viste. Soluzione ineccepibile, perché l'ambigua disposizione comunitaria è superflua se vuole riferirsi ai criteri di determinazione dell'indennizzo, altrove previsti, illogica se intende condizionare l'indennizzo, in luogo di altre misure, all'assenso della parte lesa.

La Direttiva, è stato notato, non si spinge fino al punto di definire in maniera inequivoca la natura giuridica del segreto commerciale, con gravi incertezze circa la disciplina applicabile (e conflitti possibili) in caso di attuazione con modelli diversi negli Stati membri e di violazioni transnazionali del segreto: infatti, se il segreto è qualificato atto di concorrenza sleale, varranno le regole del luogo dove è patito il danno (art. 8, par. 1 del Regolamento (CE) n. 864/2007); se il segreto

²⁶ Così, F. BANTERLE, M. BLE, *Alcune novità introdotte dalla Direttiva Trade Secrets*, cit., 202 ss.

è riguardato come diritto di proprietà intellettuale, varranno le regole del Paese nel quale la protezione è chiesta (art. 8, par. 2 del Regolamento (CE) n.864/2007)²⁷.

Ma a parte questi pur importanti aspetti, quand'anche si ritenga che la Direttiva europea sui segreti commerciali sia da ascrivere al modello c.d. concorrenziale, il suo raffronto con la disciplina (d'ispirazione proprietaria)²⁸ del *Defend Trade Secret Act* del 2016, non fa emergere differenze sostanziali²⁹. Si delinea, invece, una positiva convergenza verso il rafforzamento della tutela dei segreti³⁰, che cerca di allinearsi al mutato contesto economico, sociale, culturale e tecnologico e di dare risposta sul piano del *private enforcement* a fenomeni crescenti di criminalità da spionaggio industriale³¹.

²⁷ Evidenzia la mancanza di una scelta di fondo, V. FALCE, *Segreto commerciale, concorrenza sleale e il diritto di proprietà intellettuale. Certezze e perplessità della Dir. Ue 2016/943*, in *Dir. ind.*, 2017, 565.

Afferma, invece l'impostazione concorrenziale della Direttiva, T. APLIN, *Right to Property and Trade Secrets*, in Geiger (a cura di), *Research Handbook on Human Rights and Intellectual Property*, Elgar, 2015, pubblicato (e qui citato) su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2620999. L'A., muovendo da questa impostazione finisce per escludere che il segreto - differentemente dal marchio, brevetto e diritti d'autore - trovi protezione sotto l'art. 1 del Primo Protocollo della Convenzione Europea dei Diritti dell'Uomo e sotto l'art. 17, comma 2, Carta dei diritti fondamentali dell'Unione europea; una diversa soluzione, per suggestione con quanto accade per i diritti dell'uomo o come portato di una concezione proprietaria assolutista, porterebbe ad una interpretazione restrittiva delle eccezioni e delle cause di liceità presenti nella Direttiva, e questo «*would be likely to create pressure to apply strict liability to third parties*» (16), sull'assunto (erroneo) che la Direttiva non preveda una responsabilità oggettiva del terzo. È, invece, vero il contrario, poiché la buona fede (originaria) rileva solo, e con alcuni limiti, ai fini rimediali, come dimostrato poc'anzi nel testo.

Per la concezione proprietaria, M. BRONCKERS, N. M. MCNELIS, *Is the EU obliged to improve the protection of trade secrets? An inquiry into TRIPS, the European Convention on Human Rights and the EU Charter of Fundamental Rights*, 34 *Europ. Intel. Property Rev.* 673 (2012) e reperibile su https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1770235, con conclusioni opposte ad Aplin, nel senso che i segreti commerciali trovano collocazione tra i diritti fondamentali. Si rinviene inoltre una tabella riassuntiva dei vari regimi di tutela del segreto presenti negli Stati Membri, al 2012 (687). Cfr., anche, per la prospettiva proprietaria, L. BENTLY, *Trade Secrets: 'Intellectual Property' But Not 'Property'?*, in Howe - Griffiths (a cura di), *Concepts of Property in Intellectual Property Law*, CUP, 2013, 60-93.

²⁸ Qui si parla di *owner of a trade secret* (*Defend Trade Secrets Act of 2016*, 18 USC, § 1836(b)(1)) e ancora di *Rights of Trade Secret Owners* (*Defend Trade Secrets Act of 2016*, 18 USC, § 1835(b)), mentre nel diritto comunitario (e in quello interno italiano, art. 98, comma 1 c.p.i) si opta per la locuzione meno caratterizzante di «detentore del segreto commerciale» (*trade secret holder*, nella versione inglese, art. 2, par. 1, n. 2) Direttiva).

²⁹ Così, M. LIBERTINI, *Le informazioni commerciali riservate (segreti commerciali)*, cit., 569.

³⁰ *Ibidem*, ove le conclusioni nel senso che la «tendenza espansiva merita (...) di essere assecondata, perché le differenze di patrimonio informativo fra le diverse imprese favoriscono la differenziazione dell'offerta e la spinta verso il miglioramento della stessa» (577).

³¹ Per la protezione penale dei segreti commerciali, cfr. G. GUALTIERI, *La tutela penale del know how: la violazione del segreto industriale*, in *Dir. ind.*, 2018, ove l'analisi dei caratteri essenziali della nozione di segreto penalmente rilevante. Il terreno del segreto industriale, appena

3. *Know-how* e segreto commerciale

La Direttiva *Trade Secrets* ricomprende nell'istituto di segreto commerciale la nozione di *know-how*³², in un rapporto da *genus* a *species*, come a chiare lettere dimostra il Considerando (1) e la stessa intitolazione della Direttiva.

È meno chiaro, però, se la definizione avvenga con valenza dogmatica, con un effetto espansivo su norme dell'ordinamento che si riferiscono al *know-how* e, per osmosi inversa, con un effetto recettivo dei contenuti di queste disposizioni all'interno dello stesso concetto di segreto commerciale. Mi riferisco, ad esempio, alla definizione di *know-how* che si rinviene all'art. 1, lett. i) del Regolamento C.E. n. 772/2004 (che ha abrogato e sostituito il Reg. C.E. n. 240/96), relativo all'applicazione dell'art. 81, par. 3, TCE (ora art. 101 T.F.U.E.) a categorie di accordi di trasferimento tecnologico. Il *know-how* è definito come: «patrimonio di conoscenze pratiche non brevettate derivanti da esperienze e da prove, patrimonio che è: i) segreto, vale a dire non genericamente noto o accessibile; ii) sostanziale, vale a dire significativo e utile per la produzione di prodotti contrattuali; e iii) individuato, vale a dire descritto in modo sufficientemente esauriente, tale da verificare se risponde ai criteri di segretezza e sostanzialità»³³. Quindi, in raffronto alla definizione di segreto commerciale, sono indicati alcuni requisiti ulteriori (individualità) oppure ne difettano altri (adeguata protezione). Ancora, si consideri la definizione di *know-how* nella legge sul *Franchising* (l. n. 129/2004), che ripete quella poc'anzi ricordata, ma vi aggiunge che «il Know-how comprende conoscenze indispensabili all'affiliato per l'uso, per la vendita, la rivendita, la gestione all'organizzazione dei beni o servizi contrattuali» (art. 1, comma 3, lett. a)); si tratta di un elemento del tutto incongruo se fosse riferito alla nozione generale di segreto commerciale.

dissodato dagli studiosi di diritto industriale, è invece stato sempre elettivo per la scienza penalistica: S. GIAVAZZI, *La tutela penale del segreto industriale*, Milano, 2012; G. COCCO, *La tutela penale del segreto industriale*, in *Trattato di diritto penale dell'impresa*, diretto da A. Di Amato, IV, Milano, 1993; A. ALESSANDRI, *Riflessi penalistici dell'innovazione tecnologica*, Milano, 1984; N. MAZZACUVA, *La tutela penale del segreto industriale*, Milano, 1979; A. CRESPI, *La tutela penale del segreto e concorrenza sleale*, in AA.VV., *La repressione penale della concorrenza sleale*, Milano, 1966; ID., *La tutela penale del segreto*, Palermo, 1952.

³² In generale, sul concetto, si rinvia alle voci enciclopediche di A. FRIGNANI, *Know-how* (voce), in *Dig. it. disc. priv.*, Sez. Comm., VIII, Torino, 1992, 84 e L. SORDELLI, *Know-how* (voce), in *Enc. Giur.*, XVII, Roma, 1990, 2, nonché alle monografie di B. FRANCHINI STUFLER, *Il know-how e la tutela dei segreti d'impresa*, Torino, 2009 e F. MASSA FELSANI, *Contributo all'analisi del know-how*, Milano, 1997. Negli USA il know-how è tradizionalmente ricondotto ai *trade secrets*, v. R. M. MILGRIM, *Trade Secrets*, New York, 1987.

³³ La definizione è la stessa dell'art. 1, lett. i) del Regolamento (UE) n. 316/2014 del 21 marzo 2014 relativo all'applicazione dell'articolo 101, paragrafo 3, del Trattato sul funzionamento dell'Unione europea a categorie di accordi di trasferimento di tecnologia.

Orbene, l'elaborazione di una categoria unitaria di *know-how*, a partire dalla definizione di segreto commerciale, non avrebbe alcuna funzione euristica del diritto positivo, ed anzi, dalle poche considerazioni fin qui fatte, mi pare che complicherebbe molto l'applicazione delle norme; piuttosto migliore soluzione è quella di considerare categorie normative settoriali di *know-how*. Conforta questa opinione, l'art. 2 della Direttiva che offre la definizione di «segreto commerciale», preoccupandosi di limitarne la portata, appunto «ai fini della (...) direttiva».

4. Il segreto commerciale nel c.p.i.: il carattere aziendale dell'informazione e la tutela del *know-how* accademico

Il codice della proprietà industriale soccorre il detentore del segreto commerciale violato abusivamente *erga omnes*, contro l'autore dell'illecito e nei confronti del terzo in buona fede, seppure con un alleggerimento della sua posizione, per i previsti temperamenti rimediali.

L'art. 1 del Codice considera il segreto commerciale un diritto di proprietà industriale non titolato; onde il segreto commerciale è un bene giuridico (ed economico) da ascrivere tra i beni immateriali³⁴: non ha (più) credito, quantomeno per l'inequivoco dato di legge, l'idea che il segreto si riduca ad una mera situazione di fatto.

³⁴ Ricorrono per il segreto, a ben esaminare, le caratteristiche che la dottrina tradizionale annette al concetto di bene immateriale: necessità di estrinsecazione; trascendenza; circolarità e riproducibilità; indistruttibilità (non in senso assoluto s'intende); possibilità di un contemporaneo godimento; insuscettibilità di un immediato godimento economico (nel senso che come ogni altra produzione intellettuale trova la sua utilità economica solo con la realizzazione concreta e quindi indirettamente, attraverso un mezzo materiale, sottoposto a diversa e separata disciplina). Per queste caratteristiche, M. ARE, *Beni immateriali (dir. priv.)* (voce), in *Enc. dir.*, V, 1959, Milano, 244, e in generale, sul concetto, F. VOLTAGGIO LUCCHESI, *I beni immateriali*, Milano, 1962.

Critico nei confronti della teoria dei beni immateriali è O. T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, Milano, 1982, 458 ss. Prende le mosse dal giureconsulto Gaio, che per primo distinse tra *res corporales* ed *incorporales* alla materia delle cose in senso giuridico, G. PUGLIESE, *Dalle "res incorporales" del diritto romano ai beni immateriali di alcuni sistemi giuridici odierni*, in *Riv. trim. dir. proc. civ.*, 1982, 1137. Ma qui il giureconsulto Gaio (*Gai. Inst.*, II, 11: «*Quaedam praeterea res corporales sunt, quaedam incorporales. Corporales hae quae tangi possunt, velut fundus homo vestis aurum argentum et denique aliae res innumerabiles. Incorporales sunt quae tangi non possunt, qualia sunt ea quae jure consistunt, sicut hereditas usufructus obligationes quoquo modo contractae*») quando parla di incorporalità si riferisce ai diritti, che *tangit non possunt*, con un significato affatto diverso di quello che attualmente si riconosce per le entità intellettuali (cfr. M. ARE, *op.ult.cit.*, 244), ed a partire dalla concettualizzazione di *Immaterialgüterrechte* di Josef Kohler (*Das Atorrecht*, Jena, 1880).

Non qualsiasi conoscenza, però, è oggetto di tutela *ex artt.* 98 e 99 c.p.i. per il solo fatto d'essere riservata³⁵; per la tutela occorre (i) che la conoscenza sia una informazione aziendale (tecnico-industriale o commerciale); (ii) che soddisfi dati e necessari requisiti (di non facile accessibilità, sostanzialità, e sottoposizione a misure ragionevolmente adeguate di protezione); (iii) che sia stata acquisita o sia utilizzata da terzi, senza il consenso del legittimo detentore, «in modo abusivo» (nel diritto statunitense *misappropriation*)³⁶; (iv) che, infine, non sia possibile opporre eccezioni alla divulgazione fondate su interessi di rango superiore.

Il riferimento di legge alle «informazioni aziendali» e alle «esperienze tecnico-industriali, comprese quelle commerciali» (art. 98, comma 1), è più prosaico, meno dettagliato, di quello della corrispondente norma definitoria americana dei *Trade Secrets* (18U.S.C. §1839(3))³⁷; in entrambi i casi, però, si è di fronte ad una categoria dal contenuto aperto, di cui occorre fissare la soglia minima.

Se ci si mantiene ai dati testuali che il diritto positivo offre, e precisamente all'aggettivo «aziendale» che deve caratterizzare l'informazione, non si può parlare di segreti commerciali al di fuori di realtà imprenditoriali (si scorge in questo, un avvicinamento al modello concorrenziale). Cosicché, chi abbia ideato privatamente, con sforzi e impiego di tempo, una nuova ed efficace strategia di *marketing*, tenuta gelosamente sotto password nel proprio computer, sottratta illecitamente ed utilizzata che fosse da un soggetto economico, non potrebbe invocare le tutele del Codice p.i., bensì dovrebbe rivolgersi alle sedi penali e all'aquiliano rimedio dell'art. 2043 c.c.; escluso, in difetto di rapporto di concorrenzialità, il rimedio della concorrenza sleale³⁸.

A soluzione diversa, però, è dato pervenire per il c.d. *know-how* accademico, sulla base del primato del diritto comunitario, disapplicata la norma interna, l'articolo 98 del Codice, in contrasto con la Direttiva, non pienamente recepita. Alludo al problema della tutela reale delle innovazioni di carattere tecnologico non brevettate³⁹, risultato di ricerca all'interno dell'università o di un ente

³⁵ Sulla tutela delle informazioni riservate che non costituiscono segreti nel senso proprio del Codice, D. SBARISCA, *La tutela concorrenziale delle informazioni*, cit., 127 ss.

³⁶ 18 U.S.C., § 1839(5), che offre la definizione del termine.

³⁷ «The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (...)» (18U.S.C. §1839(3)).

³⁸ L'art. 2598 c.c. non è invocabile (neppure) dal professionista: Cass., 13 gennaio 2005, n. 560, in *Giur. it.*, 2005, n. 1177.

³⁹ Per mancanza di altezza inventiva o per scelta di non brevettare: perché l'ente di ricerca o l'università, con risorse limitate e numerosi progetti da finanziare, decide di non coprire i costi del deposito di un brevetto, di cui non appaia un qualche ritorno (in termini di opportunità di protezione, si esprime il regolamento del CNR per la generazione, gestione e valorizzazione della proprietà intellettuale sui risultati della ricerca, del 14 novembre 2013, pubblicato in G. U., serie generale n. 281 del 20/11/2013); e perché, in assenza di una copertura dei costi da parte dell'ente,

pubblico di ricerca; ed in particolare, per le problematiche di legittimazione implicate, ai risultati di ricerca c.d. autonoma o libera⁴⁰.

La Direttiva *Trade Secrets* nel definire il segreto commerciale non lo qualifica come informazione a carattere aziendale, anzi non la qualifica affatto (art. 2 Direttiva); non richiede che il detentore del segreto sia un imprenditore, bensì che possa essere «qualsiasi persona fisica o giuridica che controlla legittimamente un segreto commerciale» (art. 2, par. 1, n. 2). Utile indicazione, inoltre, dal Considerando (1) da cui si deduce che è segreto commerciale anche il patrimonio di *know-how* e di informazioni degli «enti di ricerca non commerciali»⁴¹. Infine, la necessità di salvaguardare il principio di tutela minima (cui è informata la Direttiva)⁴², conforta nella soluzione della disapplicazione della normativa interna. Quanto all'ulteriore profilo della legittimazione alla tutela del *know-how* da ricerca autonoma, dalla comunemente ritenuta eccezionalità⁴³

anche il ricercatore può essere costretto ad abbandonare l'idea di proteggere l'invenzione con brevetto. Discorso a parte è, invece, quello dell'innovazione mantenuta segreta in attesa del deposito della domanda di brevetto per evitarne la predivulgazione, nel qual caso vi sono precisi obblighi nei regolamenti accademici (A. MUSSO, *Recenti sviluppi normativi sulle invenzioni "universitarie" (con alcune osservazioni sul regime delle altre reazioni materiali)*, in *Studi di diritto industriale in onore di Adriano Vanzetti*, II, Milano, 2004, 1114, in part. nt. 135). Sul tema delle invenzioni universitarie, G. FLORIDIA, *Le invenzioni universitarie*, in *Dir. ind.*, 2007, 313, ove l'A. riporta la propria posizione sul tema della spettanza delle invenzioni derivanti da ricerca universitaria prima della Legge Tremonti, facendo distinzione tra ricerca libera e vincolata: la prima, utile per la produzione scientifica e la carriera del ricercatore, «spezza ogni collegamento tra i ricercatori di tutte le fasce e lo Stato come persona giuridica con la quale pure intercorre il rapporto di pubblico impiego», donde le invenzioni in tale contesto non sono invenzioni di dipendenti neppure riconducibili al rapporto di pubblico impiego (317).

⁴⁰ L'art. 2, Regolamento sulla proprietà industriale del Politecnico di Milano (del 7 ottobre 2011 e reperibile su https://www.polimi.it/fileadmin/_migrated/content_uploads/regolamento-sulla-proprietà-industriale-di-ateneo_01.pdf) definisce l'attività di ricerca autonoma come «attività di ricerca dell'Ateneo svolta dai dipendenti o dagli interni non dipendenti del Politecnico, sviluppata autonomamente, avvalendosi di attrezzature e strutture e/o di finanziamenti e di risorse economiche amministrare dal Politecnico»; similmente, art. 2, lett. g) del Regolamento CNR, cit..

⁴¹ Così in modo inequivoco: «Le imprese e gli enti di ricerca non commerciali investono nell'acquisizione, nello sviluppo e nell'applicazione di know how e informazioni (...). Questo prezioso patrimonio di know how e di informazioni commerciali, che non è divulgato ed è destinato a rimanere riservato, si definisce segreto commerciale» (Considerando 1).

⁴² «Gli Stati membri possono (...) fornire un livello più ampio di protezione contro l'acquisizione, l'utilizzo o la divulgazione illeciti dei segreti commerciali rispetto a quello previsto dalla presente direttiva» (art. 1, par. 1, Direttiva).

⁴³ Immediato precedente normativo è l'art. 24 bis l.inv. (abr), introdotto dall'art. 3 della legge 18 ottobre 2001, n. 383. Sul punto, G. FLORIDIA, *Le innovazioni universitarie secondo il pacchetto Tremonti*, in *Dir. ind.*, 2002, 9) che ha innovato profondamente il previgente sistema stabilendosi il principio per il quale il ricercatore è titolare esclusivo dei diritti derivanti dalle invenzioni brevettabili di cui è inventore. In controtendenza, peraltro, all'esperienza di altri Paesi: degli Stati Uniti, dove il *Bayh-Dole Act* del 1980 attribuisce la titolarità dei brevetti agli enti di ricerca, al fine di legittimare *ex lege* lo sfruttamento delle relative invenzioni; dell'ordinamento tedesco, dove il § 42 della legge 25 luglio 1957 sulle invenzioni dipendenti, che contemplava il

del principio della titolarità esclusiva in capo al ricercatore dei diritti dalle invenzioni brevettabili (l'art. 65 c.p.i. è «in deroga all'articolo 64»), si deduce che il detentore in via originaria ed *ex lege* del patrimonio di *know-how* è l'ente⁴⁴, non il ricercatore.

5. Segretezza e *reverse engineering*

Le informazioni devono essere segrete, nel senso che nel loro insieme o nella precisa configurazione e combinazione dei loro elementi non siano «generalmente note» o «facilmente accessibili» agli esperti e agli operatori del settore (art. 98, comma 1, lett. a) c.p.i.)⁴⁵. Trascurando le ipotesi d'evidenza delle informazioni generalmente note, cioè conosciute dalla maggior parte dei concorrenti, veri e propri *segreti di Pulcinella*, conviene soffermarsi sul requisito della non facile accessibilità, specie delle informazioni tecnico-industriali.

Nella prassi decisionale, tale aspetto - demandato in genere ad un accertamento tecnico in giudizio - è strettamente connesso alla verifica se l'informazione sia ricavabile attraverso un processo di *reverse engineering*⁴⁶, cioè

riconoscimento del brevetto in capo ai docenti e ricercatori universitari, è stato modificato dalla l. 18 gennaio 2002 attribuendo la titolarità in capo all'Ateneo, sia pure - a quanto pare - a titolo derivativo, cfr., A. MUSSO, *op. cit.*, 1064-1065 e nt 8.

⁴⁴ Così il regolamento del CNR, art. 2, comma 1, lett. d) cit.: «Know-how: è l'insieme delle conoscenze, codificate e non, di titolarità del CNR, derivanti dalle ricerche svolte e che non formano oggetto di specifici diritti di proprietà intellettuale. Ai fini del presente Regolamento rientrano nella definizione di know-how anche le invenzioni non brevettate» [enfasi nostra].

⁴⁵ Formulazione diversa, ma sostanzialmente coincidente nella Direttiva - «*a persone che normalmente si occupano del tipo di informazione in questione*» (art. 2, par. 1) lett. a) Direttiva - e nel U.S.C.: «*from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information*». Cfr., BONE, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, cit., 245, e in giurisprudenza, Arco Indus. Corp. v. Chemcast, 633 F.2d 435, 441 (6th Cir. 1980).

⁴⁶ *Ante* Codice p.i., per la liceità del *reverse engineering*, Trib. Verona, ord., 23 luglio 1998, in *GADI* 1998, 3831; Trib. Torino, 1 giugno 2001, in *GADI* 2001, 4295, 916; Trib. Orvieto, ord., 4 luglio 1996, in *GADI* 1996, 3499, 887. In dottrina, la liceità era subordinata alla verifica del requisito della facile accessibilità *ex art. 6 bis l.i.*, onde essa era esclusa quando il *reverse engineering* richiedeva sforzi e tempi tali per cui le informazioni potevano conseguentemente apparire come di non facile accesso (L. MANSANI, *La nozione di segreto di cui all'art. 6bis l.i.*, in *Il diritto industriale*, 2002, 217, 218; G. GUGLIELMETTI, *La tutela del segreto*, in *Le nuove frontiere del diritto dei brevetti*, Torino 2003, 119).

Dopo l'introduzione del c.p.i., e prima della novella del 2010, si era posto il tema se il *reverse engineering* costituisse o meno una forma autonoma ed indipendente di apprendimento delle informazioni: per V. FALCE, *Profili pro-concorrenziali dell'istituto brevettuale*, Milano 2008, 170, il riconoscimento del diritto esclusivo avrebbe comportato la illiceità della decompilazione dei prodotti immessi sul mercato; altra parte della dottrina considerava la tecnica del *reverse engineering* un modo indipendente per ottenere i dati segreti potendo comportare anche forme di investimento autonomo e protezione concorrente, M. BERTANI, *Proprietà intellettuale e nuove*

con l'osservazione, l'analisi chimica o l'esame meccanico scompositivo del prodotto, con tre diversi possibili esiti:

(i) il processo di decompilazione non è possibile (es. software c.d. proprietario)⁴⁷ o, seppur possibile, non consente di risalire al segreto (dall'analisi del composto chimico alla formula, dal prodotto noto al procedimento industriale ignoto, ecc.);

(ii) la decompilazione sarebbe in astratto possibile, ma con tempi e costi particolarmente elevati;

(iii) l'informazione tecnica è desumibile da mera analisi, esame, scomposizione del prodotto.

Solo in quest'ultima ipotesi, a quanto comunemente ritenuto, viene meno il requisito della segretezza, preclusa per difetto dei requisiti la tutela reale, salva la (possibile) rilevanza per concorrenza sleale⁴⁸.

Per contro, la difesa del concorrente di aver carpito il segreto di fabbricazione per *reverse engineering*, a fronte di costi elevati, non gli gioverebbe affatto: o perché non fa venire meno la segretezza, in quanto non facilmente accessibile, oppure perché sarebbe comunque da riguardare quale comportamento sleale, sanzionabile ex art. 2598, comma 3 c.c.; queste modalità, altrimenti detto, assumerebbero la connotazione di uno sfruttamento parassitario di sforzi e conoscenze altrui, con l'attribuzione di un vantaggio sproporzionato rispetto alle risorse utilizzate. Tale soluzione, nell'assetto normativo attuale, non pare condivisibile perché se si considera il carattere pro-concorrenziale che la direttiva comunitaria, pur in un contesto di rafforzata tutela, assegna a chiare lettere al segreto commerciale (Considerando 10)⁴⁹, si dovrà ammettere che l'attività di *reverse engineering* è una causa di liceità dell'acquisizione del segreto

tecniche di protezione delle informazioni, in *Studi in onore di Gerhard Schriker*, Milano, 2005, 39 il quale aggiunge che qualora non sia seguito da una divulgazione generalizzata può addirittura dare vita ad una privativa (39). La novella del 2010 pareva nuovamente liceizzare il *reverse engineering* se non sia compiuto attraverso mezzi abusivi o non sia favorito da acquisizioni illecite di informazioni, così, D. DE ANGELIS, *Informazioni segrete e diritti di proprietà industriale non titolati*, in M. Scuffi, M. Franzosi, *Diritto industriale italiano*, I, Torino, 2013, 901.

⁴⁷ Cfr., App. Torino, Sez. spec. in materia di imprese, 19 maggio 2017, in *Quotidiano giuridico*, 2017, per una fattispecie di abusivo utilizzo di un software per archiviazione di dati, in formato proprietario. Sulla tutela autoriale del codice sorgente, e quindi per l'illiceità del *reverse engineering* sotto il diverso profilo della protezione del software, G. GUGLIELMETTI, *Analisi e decompilazione*, in Ubertazzi, *La legge sul software*, Milano 1994, 164.

⁴⁸ È generalmente ammessa, per le informazioni riservate, una tutela obbligatoria (residuale) ex art. 2598, n. 3 c.c., così, Trib. Bologna, 27 luglio 2015, in *www.infojuris.it*. In dottrina, D. SBARISCIA, *La tutela concorrenziale delle informazioni "meno riservate"*, cit., 127.

⁴⁹ Come dichiarato dal Considerando 10: «nell'interesse dell'innovazione e della concorrenza, le disposizioni della presente Direttiva non dovrebbero creare alcun diritto esclusivo sul know-how o sulle informazioni che godono di protezione in quanto segreti commerciali. Pertanto, la scoperta indipendente di know-how e di informazioni resta lecita e i concorrenti del detentore del segreto commerciale sono altresì liberi di cercare il segreto di fabbricazione (reverse engineering) per qualsiasi prodotto acquisito lecitamente».

commerciale, senza alcuna limitazione di sorta per il concorrente («libero da qualsiasi obbligo giuridicamente valido» (art. 3, comma 1, lett. b), Direttiva). E se si accoglie tale prospettiva, la lettura conforme del diritto nazionale all'opzione normativa comunitaria porta a ritenere che mentre il detentore del segreto è onerato della prova della non facile accessibilità in astratto dell'informazione, il concorrente può vittoriosamente dimostrare in concreto che l'acquisizione del segreto è stata lecita, per aver condotto un'attività di *reverse engineering*, poco importa, qui, se dispendiosa, con tempi e costi particolarmente rilevanti; né può considerarsi tale condotta di per sé sola, espressione di *abusività*⁵⁰.

6. Il valore economico del segreto

L'informazione deve avere, altresì, «valore economico»⁵¹ in quanto segreta (art. 98, comma 1, lett. b) c.p.i.). La locuzione è polisemica. Con essa si può

⁵⁰ Altro discorso è quello di una pervicace opera di decompilazione che abbia rilievo quale circostanza, da valutarsi nel complesso di una condotta più ampia, come parassitaria, sleale, rilevante ex art. 2598, n. 3 c.c. Processualmente è necessaria apposita domanda di tutela del detentore del segreto, svolta in genere in via cumulata con l'azione ex art. 99 c.p.i. Sulla possibilità di cumulo delle tutele, A. VANZETTI, V. DI CATALDO, *Manuale di diritto industriale*, Milano, 2012, 117. Nel diritto statunitense si sottolinea come l'attività di decompilazione debba avvenire «*by a fair and honest means*», come ad esempio l'acquisto dell'articolo sul mercato; onde l'attività di decompilazione per essere lecita richiede una corretta acquisizione delle informazioni e il rispetto di pratiche commerciali etiche, cfr. HALT G.B., DONCH J.C., STILES A.R., FESNAK R., *Trade Secrets*, in *Intellectual Property and Financing Strategies for Technology Startups*, Springer, Cham, 2017, 147. È altresì lecita la reverse engineering in violazione di un contratto di licenza con l'utente finale, cfr. Aqua Connect Inc. v. Code Rebel, LLC et al., Case No. CV 11-5764-RSWL (C.D. Cal. 2012) (Lew, J.); Code Rebel è una società di software che dopo aver scaricato una versione di prova del software "ACTS" di Aqua Connect, ne ha invertito il codice di programma. Per Aqua Connect, Code Rebel ha sottratto il segreto commerciale; nonostante il fatto che sia necessaria la versione di prova del software ACTS accettazione di un Contratto di licenza con l'utente finale click-to-talk per accedere a programma, con uno dei termini che l'utente finale non effettuerà reverse engineering del programma: il tribunale distrettuale degli Stati Uniti per il distretto centrale della California ritiene che il software da reverse engineering in violazione di una clausola del contratto di licenza con l'utente finale, non costituisce appropriazione indebita di segreto commerciale.

⁵¹ Che può essere oggetto di appostazione in bilancio, Cass., 27 febbraio 1985, n. 1699, in *Giur.it.*, 1985, I, 889, in *Foro it.*, 1985, I, 2661, nonché in *Società*, 1985, 870: il know-how rappresentando un distinto bene economico relativo ad un'immobilizzazione di tipo immateriale se derivante da un rapporto qualificabile come concessione, va iscritto nelle poste attive del bilancio ai sensi dell'art. 2424, n. 5 c.c., e stimato per un valore non superiore al prezzo d'acquisto o di costo secondo la previsione dell'art. 2425, n. 3 c.c. Sulla conferibilità a capitale, quale conferimento in natura ex art. 2342, comma 3 c.c., L. DI LORENZO, *Conferibilità di know-how nelle società di capitali: soluzioni pratiche e tecnica contrattuale*, in *Notariato*, 2014, 455, con conclusioni non del tutto persuasive. Infatti, il dato positivo dell'art. 2343, comma 1 c.c. (nelle s.p.a) e dell'art. 2465, comma 1 c.c. (nelle s.r.l.) che fa obbligo nella relazione di stima (da allegare

alludere al vantaggio competitivo del detentore o alla sostanzialità del segreto ai fini della produzione («significativo e utile per la produzione dei prodotti contrattuali», secondo la definizione di *know-how* dell'art. 2 del Reg. UE/316/2014), oppure, con maggiore aderenza semantica, al fatto che l'informazione abbia un (qualche) valore economico per via degli investimenti in ricerca e sviluppo, dei costi di protezione, o avuto riguardo, se presente, al valore di bilancio⁵².

7. L'adozione di adeguate misure di protezione

Oltre che segrete (nell'accezione di oggettiva difficoltà a risalire all'informazione mediante decompilazione) le informazioni devono essere anche *segretate*, ossia sottoposte a misure di protezione adeguate («misure da ritenersi ragionevolmente adeguate a mantenerle segrete», art. 98, comma 1 c.p.i.). La legge non esemplifica le misure adottabili, diversamente da quanto avviene nell'art. 32 del Regolamento europeo sulla *privacy*⁵³. Nondimeno entrambe le

all'atto costitutivo) di *descrizione* del bene conferito, è insuperabile ed osta alla conferibilità del know-how (tecnico), pena la perdita della segretezza e quindi del suo valore; insufficiente (come invece ritiene il Di Lorenzo) una dichiarazione di attestazione di segretezza del titolare, incapace di fornire la tutela minima che la valutazione oggettiva di un perito fornisce. Nega la conferibilità, V. DI CATALDO, *I brevetti per invenzione e per modello*, artt. 2584-2594, in P. Schlesinger, *Codice Civile. Commentario*, Milano, 1988, 50 e nt. 105, secondo cui il conferimento di know-how sarebbe «tecnicamente impossibile»; medesima opinione anche di A. PISANI MASSAMORMILE, *Conferimenti in s.p.a. e formazione del capitale*, Napoli, 1992, 194. Per la conferibilità, ma sull'argomento non persuasivo che la relazione di stima non debba essere di dettaglio (così obliando del tutto il dato positivo, che invece impone l'obbligo della descrizione) e su quello (non decisivo) che la relazione assolva ad una funzione organizzativa, C. STRIPPOLI, *Gli apporti di know-how nelle società di capitali*, in *Dir. ind.*, 2018, 138-139. Ammette la conferibilità solo del Know-how, la cui descrizione non comporti rivelazione della composizione, G.B. PORTALE, *I conferimenti in natura "atipici"*, Milano, 1974, 3 e nt. 7: soluzione di giusto compromesso, potendo accadere che il segreto sia *aliunde* individualizzato e tale da poter essere oggetto di conferimento e così, una formula chimica segreta, oggetto di licenza o di trasferimento di tecnologia. Si consulti anche, G. OLIVIERI, *Il conferimento di know-how ed il decreto di attuazione della seconda direttiva comunitaria in materia di società*, in *Riv. soc.*, 1987, 14, il quale rinviene il divieto di conferibilità del *know-how*, nel divieto di imputazione a capitale di prestazioni di opera o di servizi, a norma dell'art. 2342, ultimo comma, c.c. (52), assumendo come ulteriore argomento a sostegno della tesi il fatto che il *know-how*, al pari del prestazioni d'opera, non è assoggettabile ad esecuzione forzata da parte dei creditori sociali.

⁵² Cass., 27 febbraio 1985, n. 1699, cit.

⁵³ L'art. 32 del Regolamento (UE) 2016/679 abbraccia il principio dell'*accountability* nell'adozione delle misure di sicurezza dei dati personali e abbandona il precedente sistema dettagliato delle misure minime; nondimeno, offre alcuni esempi di misure o caratteri che esse possono avere: 1) la pseudonimizzazione e la cifratura dei dati personali; 2) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; 3) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; 4) una procedura per testare,

discipline richiedono l'adozione di «misure adeguate», seppure a diversi fini: per evitare sanzioni, per il Regolamento sulla *privacy*, per ottenere una tutela quasi-privativa, per il Codice p.i. Tra le due discipline vi può essere sovrapposizione, quando i dati personali rappresentano per l'impresa importanti segreti commerciali; la lista clienti è un esempio eclatante⁵⁴. Per cui può legittimamente chiedersi se ed in che misura gli approdi di giurisprudenza a venire sulle due normative, potranno contemperarsi vicendevolmente. Aspetto che l'economia del presente lavoro mi consente solo di porre come tema di indagine, da sviluppare altrove.

Si è correttamente ritenuto⁵⁵ che l'adeguatezza delle misure va parametrata alle caratteristiche delle informazioni, alla struttura imprenditoriale del titolare ed allo stato del progresso tecnico⁵⁶. È generalmente affermato che la predisposizione di appositi strumenti di protezione delle informazioni assolva a una doppia funzione: soggettiva, di riconoscimento della segretezza all'interno dell'impresa; oggettiva, di tutela della segretezza nei confronti dei terzi (contro lo spionaggio industriale)⁵⁷.

Le misure da adottarsi possono essere quelle più banali, quali l'esistenza di una password che sia conosciuta solo da pochi soggetti autorizzati, il mettere sotto chiave alcuni documenti, disegni tecnici, formule rilevanti, la classificazione dei documenti e la marcatura degli stessi con inequivoca indicazione circa la loro segretezza (stampigliatura di segreto, riservato, copyright); o più complesse, come la limitazione degli accessi alla struttura, la predisposizione di badge identificativi, la frammentazione delle informazioni tra

verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

⁵⁴ Per Cass., 19 giugno 2008, n. 16744 in *Foro it.*, 2008, I, 2441 occorre, ai fini della tutela come segreto, che le informazioni riservate relative ai clienti abbiano un «profilo qualificante» per cui i dati contenuti in una *mailing-list* possono definirsi, secondo la Suprema corte, un mero schedario nominativo privo di elaborazioni qualificanti in senso aziendale. La protezione della lista clienti - raccolte di nominativi, estremi anagrafici e altre informazioni commerciali connesse - avviene, sussistendone i presupposti, su più livelli: attraverso la tutela come segreto commerciale ex artt. 98-99 c.p.i. (A. OTTOLIA, *Big Data e innovazione computazionale*, Milano, 2017, 49; cfr. anche A. VANZETTI, *La tutela "corretta" delle informazioni segrete*, cit., 95); con la tutela di tipo autoriale sulle banche dati relative a norma dell'art. 64 *quinquies* e ss. l.d.a. o di diritto connesso del costitutore della banca dati a norma dell'art. 102 bis ss. l.d.a. (A. ANDOLINA, *Tutela delle liste clienti tra concorrenza sleale, segreto industriale e banche dati*, in *Giur.it.*, 2018, 1145, nota parzialmente critica a Trib. Bologna, sez. spec. in materia imprese, 4 luglio 2017, che nega la tutela autoriale, ai sensi dell'art 102 bis l.d.a. per le banche dati "segrete" o comunque non destinate o non messe a disposizione del pubblico); e in via residuale soccorre anche l'art. 2598, n. 3 c.c. In giurisprudenza, Trib. Genova, 13 maggio 2014; Trib. Milano, 29 giugno 2015; Trib. Milano, 19 febbraio 2016; Trib. Milano, 21 maggio 2014.

⁵⁵ Con il limite della esigibilità, anche per i costi, così L. MANSANI, *La nozione di segreto di cui all'art. 6 bis l.i.*, cit., 217.

⁵⁶ S. BARBARO, *Le informazioni aziendali riservate: la scelta del codice della proprietà intellettuale*, in *Diritti esclusivi e nuovi beni materiali*, a cura di G. Resta, Milano 2011, 329.

⁵⁷ L. MANSANI, *op. cit.*, 219.

i vari soggetti del processo produttivo, la divisione delle aree produttive e via dicendo.

Sono misure di protezione, a quanto comunemente si reputa, anche gli accordi di segretezza⁵⁸ stretti con fornitori, clienti, collaboratori esterni oppure *a latere* di accordi di licenza di brevetti, contratti di *franchising*⁵⁹ o con i dipendenti, in genere all'assunzione, per quando avranno cessato il rapporto di lavoro e in funzione di rafforzamento degli obblighi di fedeltà⁶⁰ dell'art 2105 c.c.

La violazione del patto di segretezza comporta responsabilità contrattuale per inadempimento (utile la contrattazione di penali per la liquidazione del danno) e, concretando un modo abusivo di appropriazione del segreto (arg. art. 4, par. 3, lett. b) Direttiva), apre alla contestazione della responsabilità extracontrattuale, con tutela di carattere reale⁶¹.

⁵⁸ Sono valide le clausole di riservatezza perpetue, senza diritto di recesso, e oltre il venir meno degli accordi principali. Cfr., C. GALLI, *Potenziale perpetuità della tutela del know how e contrattualizzazione degli impegni di riservatezza*, in *Dir. ind.*, 2018, 113, ove l'ipotesi di *Non Disclosure Agreement* concluso in fase di trattativa, non andata a buon fine, e nel quale si può prevedere la sopravvivenza degli impegni, oltre la conclusione delle trattative stesse. Nello stesso senso, già G. AGHINA, *L'Obbligo illimitato di segretezza dei contratti di licenza di «know how»*, in *Aa.Vv., Problemi attuali del diritto industriale. Volume celebrativo del XXV anno della Rivista di diritto industriale*, Milano, 1977, 1 ove anche considerazioni sul rapporto tra l'illimitato obbligo di segretezza e divieto di illimitati vincoli per patto di non concorrenza, in violazione dell'art. 2125 c.c.

⁵⁹ B. VERONESE, *Franchising e tutela delle informazioni aziendali riservate*, in *Giur. it.*, 2008, 2749, nota critica a Trib. Torino, ord., 23 aprile 2008.

⁶⁰ Ampiamente, P. ICHINO, *Diritto alla riservatezza al segreto nel rapporto di lavoro*, Milano, 1979. V., anche, D. DI LEMMA, *La tutela delle informazioni riservate nei confronti del dipendente infedele: fedeltà, correttezza e buona fede*, in *Riv. it. dir. lav.*, 2017, II, 494, nota a Cass., 13 febbraio 2017, n. 3739 e A. ROSSI, *Software e invenzioni del dipendente, segreto aziendale, concorrenza*, in *Dir. lav.*, 1986, 1, 358.

⁶¹ In senso contrario al testo parrebbe, Trib. Torino, ord., 23 aprile 2008, cit., che ha escluso la tutela inibitoria contro l'uso e la divulgazione di alcune informazioni riservate in violazione degli obblighi di segretezza del *franchisee*, contrattualmente pattuiti nel tempo, sciolto il rapporto per inadempimento. Nella specie, pur accertata (in via sommaria) la violazione dei patti contrattuali di segretezza, il tribunale nega (e conferma la decisione in sede di reclamo) la tutela inibitoria, perché le informazioni prive dei requisiti oggettivi richiesti dall'art. 98. Dal contesto del provvedimento sembra trascurata la tutela contrattuale del segreto, che a quella extracontrattuale si affianca, imperniata sulla violazione dell'accordato divieto di utilizzazione "sleale", di divulgazione e di uso delle informazioni trasmesse (così, annota, B. VERONESE, *op. cit.*, 2750). Su questione sostanzialmente analoga (intercorsa tra lo stesso *franchisor* ed altro ex affiliato), la sezione specializzata del tribunale di Torino esprime orientamento opposto: v. ordinanza in fase cautelare, Trib. Torino, 12 ottobre 2007, *Magica s.r.l. c. Falco s.r.l.*, in www.osservatorino.it/documenti, poi confermata in sede di reclamo, Trib. Torino, 6 dicembre 2007, *Falco s.r.l. c. Magica s.r.l.*, in www.osservatorino.it.

Ante Codice p.i. si è giudicato che la tutela del *franchisor* contro le violazioni dell'obbligo di riservatezza del *franchisee* fosse da ricondurre, oltre che alla responsabilità per inadempimento, alla disciplina della concorrenza sleale (Trib. Milano Rho, 10 febbraio 2002, in *Riv. dir. ind.*, 2003, II, 148, con nota di BOCHICCHIO; Trib. Verona, 17 dicembre 1996, in *Giur. dir. ind.*, 1997, 467; Trib. Orvieto, 4 luglio 1996, *ivi*, 887; Trib. Milano, 6 giugno 1985, *ivi*, 1985, 613).

8. Limiti alla tutela del segreto commerciale

La scelta di tenere riservate alcune informazioni aziendali e di farne uso in regime di segretezza costituisce espressione della libertà d'iniziativa economica⁶² (art. 41, comma 1 Cost.); essa però entra, quasi fatalmente, in conflitto con altri diritti e libertà; si pensi alla stessa iniziativa economica dei concorrenti, alla promozione e diffusione delle conoscenze, al diritto alla mobilità nel lavoro, all'esercizio delle libertà sindacali o al diritto all'informazione.

In proposito, la Direttiva *Trade Secrets* introduce dei limiti alla tutela del segreto definiti ora cause di liceità, all'art. 3 ed ora eccezioni, all'art. 5. In particolare la tutela del legittimo detentore cede di fronte:

- a) alla scoperta del segreto in modo indipendente e autonomo (art. 3, par. 1, lett. a) Dir. e art. 99, comma 1 c.p.i.) o per decompilazione del prodotto, c.d. *reverse engineering* (art. 3, par. 1, lett. a) Dir.). In capo al legittimo detentore del segreto commerciale, infatti, non è ravvisabile un diritto di esclusiva assoluto. E' possibile un uso simultaneo dello stesso, quando il concorrente scopre autonomamente il segreto di fabbricazione o per *reverse engineering*. Può anche accadere che il concorrente ottenga valido brevetto (in genere si tratta di segreti di procedimento, non facilmente accessibili tramite *reverse engineering*), per cui - ed è questo un bilanciamento a favore del titolare del brevetto - il detentore del segreto non lo perde del tutto ma ne ha un limitato godimento (talvolta non sufficiente a recuperare i costi di investimento). È il diritto al preuso, riconosciuto in quasi tutti gli ordinamenti, a contemperamento degli effetti del principio del *first to file*⁶³.
- b) all'esercizio del diritto alla libertà di espressione e di informazione⁶⁴ (art. 5, par. 1, lett. a) e art. 3, par. 1, lett. c) Dir.);

⁶² A. FRIGNANI, *Segreti d'impresa* (voce), in *Dig. it. disc. priv.*, Sez. Comm., XIII, Torino, 1996, 337 ss. che critica quella tendenza dottrinale che - facendo leva sui dai principi di libera circolazione delle conoscenze ed sul rispetto degli obiettivi del diritto brevettuale - legge in modo restrittivo le norme di tutela del segreto. Per la copertura *ex art. 41 Cost.*, cfr. P. AUTERI, *Il segreto industriale relazione al Convegno Il segreto nella realtà giuridica italiana, Roma 26-28 ottobre 1981*, Padova, 1983, 328.

⁶³ L. GIOVE, A. COMELLI, *Limiti al preuso e tutela del know-how segreto*, in *Dir. ind.*, 2012, 49, nota del *leading case* sul diritto al preuso, Cass., 5 aprile 2012, n. 5497. Negli Usa i *prior user rights* sono stati riconosciuti dal *Leahy-Smith America Invents Act* del 2011, proprio in occasione dell'abbandono della regola *first to invent* in favore del *first to file*. Cfr., G. GUGLIELMETTI, *La riforma della legge americana sui brevetti adotta la regola del first to file*, in *Riv. dir. ind.*, 2012, I, 121.

⁶⁴ Sulla inevitabilità di un tale scontro, D.E. BAMBAUER, *Secrecy is Dead - Long Live Trade Secrets* 93 *Denver University Law Rev.* 833 (2016), il quale porta ad esempio la pratica del *fracking*, ossia la pratica delle compagnie energetiche di estrazione del gas naturale con l'iniezione di sostanze chimiche nel sottosuolo. L'opinione pubblica ha accusato che le sostanze chimiche

- c) alla rivelazione di una condotta scorretta, di un'irregolarità o di un'attività illecita, «a condizione che il convenuto abbia agito per proteggere l'interesse pubblico generale» (art. 5, par. 1, lett. b) Dir.) (c.d. eccezione da *whistleblowing*);
- d) alla divulgazione da parte dei lavoratori ai rappresentanti sindacali di notizie dell'azienda, pur con alcune stringenti cautele e cioè che ciò avvenga nell'ambito del legittimo esercizio delle funzioni sindacali, conformemente al diritto dell'Unione e al diritto nazionale, e a condizione che la divulgazione sia necessaria per l'esercizio delle funzioni sindacali (art. 5, par. 1, lett. c) Dir.);
- e) a un «legittimo interesse riconosciuto dall'Unione o dal diritto nazionale» (art. 5, par. 1, lett. b) Dir.); locuzione che impedisce di concepire il segreto commerciale alla stregua di un diritto proprietario con tutela assoluta.

Si consideri, a tal ultimo proposito, il rapporto tra interesse del mercato alla più ampia *disclosure* e interesse della società quotate al segreto di informazioni *price sensitive*, quali i piani e le strategie future dell'impresa, i dettagli di prodotti in progettazione o le date di loro lancio⁶⁵. Queste informazioni hanno un valore competitivo: consentono alla società, se tenute segrete, di sfruttare l'effetto sorpresa legato a date operazioni, ed impedire, in tal modo, ai concorrenti di adottare misure di contrasto efficaci. A quanto generalmente si reputa, l'obbligo (senza indugio, come impone l'art. 114, comma 1 TUF) di *disclosure* prevale sull'interesse alla segretezza⁶⁶; soluzione alla quale si può consentire, essendoci

comportano rischi significativi per la salute, ma le compagnie energetiche hanno rifiutato di divulgare le loro formule, anche alle autorità pubbliche, invocando il segreto commerciale (H. WISEMAN, *Trade Secrets, Disclosure, and Dissent in a Fracturing Energy Revolution* 111 Colum. L. Rev. Sidebar 1 (2010)). Cosicché, un privato cittadino o un dipendente che rendesse pubblica la formula, o un giornale che la pubblicasse, potrebbe essere chiamato a rispondere per *misappropriation*; ma ciò, afferma Bambauer, implicherebbe immediatamente l'appello al Primo Emendamento, specialmente se i rischi per la salute risultassero reali.

⁶⁵ S. GILOTTA, *Trasparenza e interesse societario al segreto, quale equilibrio?*, in *Analisi giur. econ.*, 2013, 255, citando A. LASHINSKY, *The Secrets Apple Keeps*, in *Fortune*, 6 febbraio 2012, ricorda come Apple sia maniacale nel modo con cui conserva il segreto sui prodotti in progettazione, loro caratteristiche e date di lancio.

⁶⁶ V., *ex multis*, C. ANGELICI, *Note in tema di informazione societaria*, in Aa.Vv., *La riforma delle società quotate. Atti del Convegno di Studio. S. Margherita Ligure, 13-14 giugno 1998*, Milano, 1998, 263; R. COSTI, L. ENRIQUES, *Il mercato mobiliare*, Padova, 2004, 213; R. LENER, *La diffusione delle informazioni «price sensitive» fra informazione societaria e informazione riservata*, in *Società*, 1999, 142; A. PERRONE, *Informazione al mercato e tutele dell'investitore*, Milano, 2003, 174 s.

Più possibilista parrebbe, P. MONTALENTI, “*Disclosure*” e riservatezza nei mercati finanziari: problemi aperti, in *Analisi giur. econ.*, 2013, 245, per il quale il «mito del *market egalitarianism* e della *market transparency* non può soffocare la competizione concorrenziale e la tutela ragionevole dei vantaggi giustificati dagli *information costs*». Cfr., anche, M. BERTANI, *Big data, proprietà intellettuale e mercati finanziari*, in V. Falce, G. Ghidini, O. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018, 39, che tratta il tema se ed in che misura le informazioni borsistiche (*pre-trade* e *post trade*) siano segreti commerciali.

al fondo una libera scelta del soggetto economico. Qualsiasi società all'atto di quotarsi fa una comparazione tra costi e benefici: deve valutare se i vantaggi connessi all'accesso ai mercati regolamentati (minor costo del capitale) siano giustificati dai maggiori obblighi di trasparenza che la quotazione comporta. Tuttavia esistono situazioni nelle quali la comunicazione al pubblico può essere ritardata, e ciò accade quando viene in gioco la stessa solidità finanziaria dell'emittente (art. 109 *ter* Regolamento emittenti)⁶⁷, come dimostra l'affaire *Kerviel-Société Générale*⁶⁸.

Un ulteriore rapporto che crea difficile bilanciamento è quello tra il diritto di accesso *ex art. 22*, l. n. 241/1990 per ottenere la documentazione necessaria per la tutela giurisdizionale, e l'interesse altrui a mantenere segrete le informazioni di carattere industriale e commerciale, contenute nei documenti; gran parte del contenzioso riguarda l'accesso agli atti di gara, da parte di chi abbia partecipato ad un appalto pubblico e sia stato escluso o abbia perso l'appalto⁶⁹. Secondo i giudici di palazzo Spada escluso il diritto di accesso illimitato ad atti e documenti, il bilanciamento andrebbe fatto dalla p.a. che rende ostensibile, in presenza di segreti commerciali, solo la documentazione «strettamente

⁶⁷ A norma dell'art. 109 *ter*, comma 2, lett. a) Regolamento emittenti Consob (delibera n. 11971 del 14 maggio 1999 e succ. modd.) costituisce circostanza rilevante che giustifica il ritardo della comunicazione quella «nel caso in cui la solidità finanziaria dell'emittente sia minacciata da un grave ed imminente pericolo». Sicché «la comunicazione al pubblico delle informazioni può essere rinviata per un tempo limitato, qualora essa rischi di compromettere gravemente gli interessi degli azionisti esistenti o potenziali, in quanto pregiudicherebbe la conclusione delle trattative miranti ad assicurare il risanamento finanziario a lungo termine dell'emittente».

⁶⁸ Riportato da S. GILOTTA, *ibidem*. Il trader Jérôme Kerviel, aggirando i sistemi di controllo interni della banca, creò una esposizione di 50 miliardi di euro superiore allo stesso patrimonio netto di Société Générale; l'esposizione da operazioni di *futures* su indici e titoli veniva coperta con fittizie operazioni di *hedging*. Tra venerdì 18 e sabato 19 gennaio 2008 le irregolarità vennero scoperte da alcuni funzionari. La settimana dopo la società pose in essere massicce operazioni di *unwinding* (liquidazione) realizzando una perdita record di 5 miliardi, azzerando l'utile di bilancio e costringendo ad un aumento di capitali. L'informazione era *price sensitive*, ma se fosse stata comunicata senza indugio al pubblico la solidità finanziaria dell'emittente sarebbe stata minacciata da prezzi punitivi di liquidazione dei derivati. Cfr., anche, F. CAPOZZI, *Banche, Société Générale condannata a risarcire 450mila euro all'ex trader Kerviel: "Licenziato senza causa reale"*, *Fatto quotidiano*, 7 giugno 2016, che dà la notizia che l'istituto bancario è stato però condannato a risarcire Kerviel, licenziato ingiustamente perché l'istituto sarebbe stato perfettamente al corrente delle operazioni fittizie dell'ex dipendente.

⁶⁹ M. BEONI, *Accesso agli atti di gara e tutela dei segreti commerciali delle imprese*, reperibile su <http://www.altalex.com/index.php?idstr=24&idnot=50219>; R. PROIETTI, *Segreti tecnici e commerciali, non sono un limite*, in *www.ilquotidianogiuridico.it*, 2010, nota a Tar Campania, sez. VI, 25 marzo 2010, n. 1657; F. BOTTEON, *Accesso difensivo alle offerte tecniche dei concorrenti e segreto industriale-commerciale: tutto da rifare in giurisprudenza dopo il d.lgs. n. 53/2010?*, in *Contratti Stato e enti pubbl.*, 2010, 406, nota a T.a.r. Puglia, sez. I, 27 maggio 2010, n. 2010; S. D'AMANO, *Appalti pubblici: tutela delle informazioni riservate e diritto ad un equo processo*, in *Rass. avv. Stato*, 2008, fasc. 2, 203, nota a Corte di giustizia, 14 febbraio 2008, C-450/06; P. PALLARO, *Diritto di accesso ai documenti pubblici e protezione di informazioni riservate nel diritto comunitario*, in *Dir. comun. scambi internaz.*, 2001, 435.

indispensabile ad assicurare la tutela degli interessi»⁷⁰ del richiedente; questa soluzione però dimostra il suo limite, in quelle situazioni in cui la p.a. finisce per selezionare il materiale difensivo della controparte di un giudizio, in essere o prevedibile.

La Direttiva chiarisce che nessuna disposizione è da intendersi come giustificazione per limitare la mobilità dei dipendenti⁷¹; essa non offre giustificazioni per limitare l'utilizzo, da parte dei dipendenti, di informazioni che non costituiscono segreto commerciale; o di esperienze e competenze acquisite in maniera onesta nel normale svolgimento del lavoro; né consente di imporre ai dipendenti, nei loro contratti di lavoro, restrizioni aggiuntive rispetto a quelle (già) consentite a norma del diritto dell'Unione o del diritto nazionale (art. 2, par. 3, Dir.).

Vi è infine il bilanciamento tra la tutela del segreto commerciale e i principi del giusto processo. L'azione in giudizio per difendere un segreto non è mai facile, anche per il rischio di una divulgazione ulteriore all'esterno che distrugge del tutto il segreto che si intende tutelare, oppure perché nel tutelare il segreto, il concorrente apprende altre informazioni aziendali riservate. In attuazione dell'art. 9 Dir., è stato inserito nel codice p.i. l'art. 121 *ter* che consente al giudice di emettere un provvedimento di divieto di utilizzo o rivelazione dei segreti commerciali contro i soggetti che a vario titolo intervengono nel procedimento giudiziario: soggetti nominati o delegati dal giudice, parti e loro rappresentanti

⁷⁰ Così, Cons. Stato, sez. VI, 18 settembre 2013, n. 4653, su decisione circa la legittimità di una richiesta di diritto di accesso avanzata da alcuni gestore locali di rete; l'accesso riguardava documenti relativi ad un sistema di metodologia per la valorizzazione del capitale investito nelle reti di distribuzione elettrica (incidente sulle tariffe), segretato dall'Autorità per l'Energia Elettrica e il Gas.

⁷¹ Che è diritto al perseguimento di posizioni migliori o legittimo interesse ad intraprendere un'attività d'impresa per conto proprio, così, A. FRIGNANI, *op.cit.ult.*, il quale offre un chiaro e completo quadro delle diverse soluzioni del conflitto. Prevale l'interesse dell'imprenditore alla segretezza, per tutta la durata del rapporto di lavoro, nel rispetto del *duty of confidence*, negli ordinamenti di *common law*, o in forza di specifico obbligo di fedeltà, quasi sempre positivizzato negli ordinamenti di *civil law*, e da noi nell'art. 2105 c.c. Invece, all'oggettiva difficoltà di bilanciamento una volta cessato il rapporto di lavoro, soccorrono (nei vari ordinamenti) alcuni criteri: (i) quello della natura delle notizie ottenute, distinte tra soggettive ed oggettive (le prime appartenenti alla preparazione culturale e professionale dei dipendenti, liberamente oggetto d'uso da parte dell'ex lavoratore); (ii) oppure al criterio che conduce al riconoscimento della liceità quando le notizie non siano ottenute in modo scorretto; (iii) o, ancora, quello dello scopo in vista del quale l'ex dipendente si è procurato determinate informazioni segrete. In giurisprudenza, da ultimo, Cass., 11 ottobre 2002, n. 14479, in *Giur.it.*, 2003, 288, secondo la quale le capacità professionali acquisite nel corso ed a causa dell'esperienza lavorativa, costituiscono parte indistinguibile della personalità del lavoratore, la cui tutela ha valore costituzionale, e ben possono, da questi, essere utilizzate per favorire la propria crescita professionale, sia alle dipendenze di altri imprenditori, sia in una propria iniziativa imprenditoriale. La tensione tra tutela dei segreti e diritto alla mobilità del lavoro è avvertita anche in altri ordinamenti, cfr., A. WAKS, *Where the Trade Secret Sits: How the Economic Espionage Act*, cit., 395.

e consulenti, difensori, personale amministrativo, testimoni e più in generale altri soggetti che a qualunque titolo hanno accesso alle notizie riservate. La violazione del provvedimento è punita dall'art. 388, comma 3 c.p. (fattispecie delittuosa introdotta dall'art. 9, d.lgs. n. 63/2018). La riservatezza è garantita nel processo e *oltre il processo*: l'ordine rimane anche dopo la definizione del procedimento e può essere disposto l'oscuramento o l'omissione delle parti contenenti i segreti commerciali nei provvedimenti che definiscono il procedimento (cautelare o di merito) e resi disponibili «anche a soggetti diversi dalle parti» (art. 121 ter, comma 3, lett. b) c.p.i.). Il potere del giudice di secretare (cioè di non rendere disponibili ad una delle parti in causa) documenti o parte di essi contenenti segreti commerciali, e più in generale, informazioni riservate, si rinviene nell'art. 121, comma 3 c.p.i.: il giudice, nell'assumere i provvedimenti di attivazione della *discovery*, adotta le misure idonee a garantire la tutela delle informazioni riservate, sentita la controparte⁷².

9. L'eccezione da whistleblowing

L'eccezione da *whistleblowing*⁷³ rende inoperante la tutela reale del segreto contro il concorrente (art. 5, par. 1, lett. b) Dir.); e, sotto altro e connesso profilo, libera il dipendente *whistleblower* dall'obbligo di fedeltà⁷⁴ (art. 2105 c.c. e art. 3, comma 1, L. n. 179/2017), illegittimo e nullo ogni atto discriminatorio o ritorsivo

⁷² Misure da individuarsi, nel rispetto del contraddittorio, caso per caso e così, M. SCUFFI, M. FRANZOSI, *Diritto industriale italiano*, II, Padova, 2013, 1323..

⁷³ Sul tema, S. FORTUNATO, *Il whistleblowing nella prospettiva del sistema di controllo interno*, in *Riv. dott. comm.*, 2017, 397. Per il rapporto con il diritto della concorrenza, A. FRIGNANI, *Il Whistleblowing nella concorrenza: la commissione elimina un ostacolo alla sua espansione*, in *Dir. ind.*, 2017, 413, e, dello stesso Autore, *Finalmente una legge generale su whistleblowing: luci ed ombre*, *ivi*, 2018, 51. Per gli aspetti penali, G. AMATO, *Profili penalistici del whistleblowing: una lettura comparatistica dei possibili strumenti di prevenzione della corruzione*, in *Riv. trim. dir. pen. economia*, 2014, 549. La Suprema corte (Cass. pen., 31 gennaio 2018, n. 9041) ha giudicato utilizzabile, quale grave indizio di reato, utile per l'autorizzazione delle intercettazioni, il contenuto della segnalazione del *whistleblower*, senza incorrere nel divieto di utilizzo delle fonti anonime (art. 333, comma 3 c.p.p.), in quanto l'identità del denunciante è nota, pur essendo coperta da riserbo al fini di tutelare il dipendente (nella specie pubblico). Per una analisi, con attenzione ai profili lavoristici, M. MARTONE, *La repressione della corruzione e la tutela del whistleblower alla luce della l. 30 novembre 2017, n. 179*, in *Arg. dir. lav.*, 2018, 61.

⁷⁴ In generale, sull'obbligo al segreto del lavoratore, v. P. ICHINO, *Diritto alla riservatezza al segreto nel rapporto di lavoro*, Milano, 1979. Nella contrattazione collettiva nazionale, generalmente, s'impone al lavoratore l'obbligo di conservare «assoluta segretezza» sugli interessi dell'azienda: art. 53, C.C.N.L. del 14 maggio 1994, per i lavoratori della piccola e media industria chimica e settori accorpatis. Analoghe previsioni: art. 71 C.C.N.L. del 5 aprile 2017, per i dipendenti delle aziende esercenti l'industria conciaria, Contratto collettivo nazionale di lavoro; art. 67, C.C.N.L. per i dipendenti delle aziende esercenti le industrie alimentari del 5 febbraio 2016, art. 1, C.C.N.L. del 26 novembre 2016, per i dipendenti delle industrie metalmeccaniche private e della installazione di impianti.

a motivo della segnalazione. Come già visto, l'eccezione trova formulazione all'art. 5 (par. 1, lett. b) della Direttiva, che è norma a carattere cogente: l'art. 1, par. 2, Direttiva *Trade secrets* impone agli Stati membri di «assicurare il rispetto» dell'articolo 5. Tuttavia il legislatore italiano non ha accolto (in modo espresso) in seno al codice di p.i. l'eccezione, né è da credere che essa si esaurisca nella disciplina nazionale, già vigente, per la tutela dei lavoratori che abbiano segnalato fatti di reato o irregolarità di cui siano venuti a conoscenza nell'ambito del proprio rapporto di lavoro, pubblico o privato (l. 30 novembre 2017, n. 179)⁷⁵. Questa legge, infatti, in confronto all'eccezione in esame, presenta un ambito di applicazione più ristretto (prevede un elenco di reati)⁷⁶, limitazioni soggettive (esistenza di un rapporto di lavoro tra segnalatore e segnalato, con esclusione di protezione per il terzo concorrente)⁷⁷, condizioni e limiti alle modalità di denuncia⁷⁸ non previsti dal diritto comunitario. Soluzione migliore è quella,

⁷⁵ La stretta lettura, tra l'art. 5 Direttiva e la legge n. 179/2017, è fatta invece dal Frignani (*Finalmente una legge*, cit., 56), il quale pure dubita (cfr. p. 54, in part. nt. 18), condivisibilmente, dell'efficacia della legge nazionale per l'assenza di seri incentivi economici alla denuncia; quali una promozione o una ricompensa, come nel modello Usa, ove la ricompensa può essere calcolata su quanto la denuncia abbia fatto incassare allo Stato o risparmiare all'autorità inquirente nell'accertamento dell'illecito. Così, Y. GIVATI, *A Theory of Whistleblowing Rewards*, in 45 *Journal of Legal Studies*, 43 (2016) che riporta alcuni dati: nel 2014, la SEC ha corrisposto ai *whistleblowers* più di \$ 30 milioni; nel 2012, l'*Internal Revenue Service* (IRS) ha ricompensato con \$ 104 milioni un *whistleblower* per la denuncia degli schemi di UBS, usati per incoraggiare i cittadini americani a evadere le tasse.

⁷⁶ Sono gli stessi per i quali è contestabile la responsabilità amministrativa dell'ente ex d.lgs. n. 231/2001. Critica la soluzione normativa, A. FRIGNANI, *op.ult.cit.*, 56.

⁷⁷ A. FRIGNANI, *ivi*, che critica la visione laburistica della legge (n. 179/2017) che richiede che l'illecito venga denunciato da chi ne è venuto a conoscenza in ragione del proprio rapporto di lavoro, lasciando senza protezione la denuncia di un terzo o di un concorrente o di un agente senza rappresentanza; per contro, legislazioni più avanzate, fanno ricorso al *whistleblower* nel diritto antitrust, per colpire gli illeciti anticoncorrenziali, ed incentivando la denuncia con programmi di clemenza (la disciplina antitrust USA prevede la *Corporate Leniency Policy* e la *Individual Leniency Policy*; analoghe regole in Inghilterra con il *Competition Act* del 1998 e l'*Enterprise Act* del 2002 (57), cfr., anche, M. MARTONE, *op.cit.*, 33. I dati positivi che confortano la tesi dell'impianto laburistico della legge, sono inequivoci; a partire dal titolo della legge. Occorre che si tratti di fatti di cui il dipendente o collaboratore sia venuto a conoscenza «in ragione delle funzioni svolte» (art. 6 comma 2 bis, lett a) d.lgs. 231/2001 come introdotto da art. 2 l. 179/2017); ed è stabilito, onde limitare il concetto di rapporto di collaborazione rilevante, che colui che abbia fatto segnalazione di fatti venuti a conoscenza in ragione di un rapporto di consulenza professionale o di assistenza con l'impresa, risponde del reato di rivelazione di segreto professionale (art. 622 c.p.) e di segreto commerciale (art. 623 c.p.) (art. 3, comma 2, l. n. 179/2017). Certamente non potrà invocare la causa di giustificazione il terzo concorrente.

⁷⁸ Nel settore privato, la legge è assai timida e parca d'indicazioni, dando luogo a incertezze ineludibili. Essa si limita a prevedere che, ai fini della protezione, il dipendente debba fare denuncia «nelle forme e nei modi» previsti, facendo cioè uso di canali (interni) che assicurino l'anonimato e da disciplinare nei modelli di organizzazione; di regola, il flusso informativo dovrebbe essere a favore dell'organismo di vigilanza, soggetto deputato per legge (art. 6, comma 2 d.lgs. n. 231/2001) a ricevere le informazioni di reato (cfr. il "Management System Guideline Anti-Corruzione" di Eni S.p.a. approvato dal Consiglio di Amministrazione di Eni spa il 29

invece, di valorizzare la clausola dell'acquisizione o rivelazione «in modo abusivo» - contenuta nell'art. 99 c.p.i. - la cui elasticità consente al giudice di recuperare l'eccezione da *whistleblowing* mediante una interpretazione conforme del diritto nazionale al diritto comunitario⁷⁹; purché ciò avvenga con prudenza per non ampliare eccessivamente la portata dell'eccezione (non si nega che abbia contenuto indeterminato, basti pensare al concetto assai vago di «condotta scorretta»): necessaria, dunque, la denuncia di fattispecie delittuose a tutela di bene giuridico⁸⁰ di natura pubblicistica e astretto da interesse generale, irrilevante la qualità del soggetto destinatario (autorità giudiziaria, organismo di vigilanza interno, giornalista), non necessario il rapporto di subordinazione con il segnalato.

ottobre 2014). Nulla però è detto nel caso in cui difetti la regolazione dei canali e circa la denuncia fatta direttamente all'autorità giudiziaria. E della cui valenza scriminante non è da dubitare per due essenziali considerazioni: essa è prevista nel settore pubblico e bisogna garantire, poi, l'effettività alla disciplina, diversamente frustata in tutti i casi (la stragrande maggioranza) in cui il dipendente abbia il timore che la segnalazione interna, non assicurando in concreto alcun anonimato, lo esponga a ritorsioni e pressioni; e metta il datore di lavoro "avvertito" nella condizione di insabbiare, e così col rischio per il lavoratore di ritrovarsi con una denuncia alla prova dei fatti infondata e licenziato, senza protezione.

⁷⁹ Il giudice interno ha l'obbligo, in assenza di misure nazionali di trasposizione di una direttiva, di interpretare il diritto nazionale quanto più possibile alla luce del tenore letterale e della finalità della direttiva: *ex multis*, Corte di giustizia, 24 gennaio 2018, causa C-616/16 e Cass., sez. un., ord., 10 febbraio 2010, n. 2906 (oggetto di molte pubblicazioni e note in *Foro.it.*, I, 2488 con nota di TRAVI, in *Corr. giur.*, 2010, 741, nota di D'ANGELO; in *Foro amm. - Cons. Stato*, 2010, 279; in *Urb. app.*, 2010, 421, con nota di LAMBERTI, CALVO; in *Riv. giur. edil.*, 2010, I, 387, con nota di SANTORO, in *Giust. civ.*, 2011, I, 205, in *Riv. trim. app.*, 2010, 1133, con nota di MANGANI); e per la quale l'interpretazione orientata comunitariamente è anzitutto obbligo d'interpretazione conforme alla Costituzione: riecheggia qui l'eco della teorica dualistica degli ordinamenti, italiano e comunitario.

Sui controlimiti al primato del diritto comunitario, che si deve arrestare di fronte ai principi supremi dell'ordine costituzionale italiano, M. GAMBARELLA, *La sentenza Taricco 2: obbligo di disapplicazione in malam partem "a meno che" non comporti una violazione del principio di legalità*, in *Cass. pen.*, 2018, 114. La *sentenza Taricco 2* risponde a Corte di Giustizia, Grande sez., 5 dicembre 2017, causa C-42/17, su questione pregiudiziale sollevata dalla Corte costituzionale (ord. n. 24/2017, in *Cass. pen.*, 2017, 1334); mentre la *prima sentenza Taricco* corrisponde a Corte di giustizia, Grande sez., 8 settembre 2015, causa C-105/14.

⁸⁰ In generale, sul tema del bene giuridico cfr.: F. BRICOLA, *Teoria generale del reato* (voce), in *Nuovissimo dig. it.*, XIX, Torino, 1974, 14 ss.; E. MUSCO, *Bene giuridico e tutela dell'onore*, Milano, 1974, 55; F. ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983 G. FIANDACA, *Il «bene giuridico» come problema teorico e come criterio di politica criminale*, in *Riv. it. dir. proc. pen.*, 1982, 42. E più di recente, D. PULITANÒ, *Offensività del reato (principio di)* (voce), in *Enc. dir., annali*, VIII, 2015, Milano, 665, secondo cui, quale sia l'interesse obiettivamente correlabile a ciascuna norma penale, lo si desume dal contenuto delle fattispecie. L'organizzazione formale di un codice e il sistema degli interessi tutelati non necessariamente coincidono, con ciò distaccandosi dalla idea più tradizionale e affermata dal legislatore storico (Relazione al Re, Lavori preparatori del codice penale e del codice di procedura penale, XII, Roma, 1930, 9).

10. Qualche riflessione finale

Il Bone (oppositore della concezione proprietaria)⁸¹, in un recente scritto, constata l'importanza sempre più crescente dei *Trade Secrets*, guardati fino ai tempi recenti come oggetto misterioso, un *brutto anatroccolo*⁸² del diritto della proprietà intellettuale; fa eco l'opinione del Bambauer⁸³: «*the future of intellectual property is in trade secrets*»: così preconizzata la definitiva perdita di importanza del brevetto. Questo scenario non è del tutto veritiero, in quanto non tutte le informazioni sono brevettabili e neppure si può dire che la scelta tra brevettazione e uso in regime di segretezza in termini alternativi sia l'unica possibile⁸⁴. Sempre più spesso, i consulenti di proprietà industriale indirizzano verso una soluzione di complementarità⁸⁵: descrivere nella domanda di brevetto giusto quanto sufficiente per passare l'esame dei controllori e tenere segrete altre informazioni, necessarie per il processo produttivo, ed altrettanto importanti ed essenziali di quelle divulgate.

⁸¹ Nello scritto, *A New Look at Trade Secret Law: Doctrine in search of Justification*, in 86 *California Law Rev.*, 245-246 (1998) definisce la *Trade Secret Law* una legge parassitaria, priva di una sua autonomia e giustificazione funzionale (246); ed esprime la convinzione, dopo aver criticato le ragioni politiche e gli argomenti di efficienza economica generalmente portati per sostenere l'utilità della tutela dei segreti commerciali, che la tutela debba essere lasciata alla contrattazione delle parti.

⁸² R. G. BONE, *Trade secrecy, innovation and the requirement of reasonable secrecy precautions*, in R. C. Dreyfuss e K. J. Strandburg (a cura di), *The Law and Theory of Trade Secrecy*, Cheltenham (UK), 2011, 46: «*Trade secret law is the ugly duckling of intellectual property*». Del resto, la nostra manualistica classica non riserva al tema che poche e scarse pagine.

⁸³ Così, D.E. BAMBAUER, *Secrecy is Dead - Long Live Trade Secrets*, in 93 *Denver University Law Rev.*, 833 (2016). Sottolineano l'importanza economica dei *trade secrets*, M. A. EPSTEIN, S. D. LEVI, *Protecting Trade Secret Information: A Plan For Proactive Strategy*, 43 *Bus. Law*, 887, 887 (1988); sostengono l'efficacia della legge sui segreti industriali, D. FRIEDMAN, W. M. LANDES, R. A. POSNER, *Some Economics of Trade Secret Law* 5 *J. Econ. Persp.* 61, 62 (1991); per l'importanza di una tutela dei segreti nell'industria informatica, G. R. PETERSON, *Trade Secrets in an Information Age* 32 *Hous. L. Rev.* 385, 386-87 (1995). D. E. BAMBAUER, *op.cit.*, indica alcuni motivi e circostanze del successo del segreto negli USA: (i) l'ampliamento dell'arte nota (in passato si considerava lo stato della tecnica solo ciò che era accessibile nel territorio degli Stati Uniti); (iv) l'aumento dell'ambito temporale dell'arte nota; (iii) nel settore medico, la mancanza di responsabilità per i medici che praticano metodi chirurgici brevettati (35 U.S.C. § 287(e) (2012)); (v) l'orientamento di alcuni tribunali che hanno introdotto eccezioni alla brevettazione, rispetto alle invenzioni *products of nature*.

⁸⁴ In termini di scelta alternativa, tra protezione brevettuale e uso in regime di segretezza, v. D. D. FRIEDMAN, W. M. LANDES, R. A. POSNER, *Some Economics of Trade Secret Law*, cit..

⁸⁵ Che ha anche una sua rilevanza giuridica, atteso che fin da Reg. CEE n. 2349/84 relativo all'applicazione dell'art. 85, par. 3 del Trattato di Roma a categorie di accordi di licenza di brevetto, si introduce il concetto di Know-how c.d. «accessorio», al fine di estendere, appunto, il campo di applicazione agli accordi muniti di clausole relative alla «cessione o concessione di conoscenze tecniche non divulgate che permettono una migliore utilizzazione dei brevetti concessi», cfr., G. OLIVIERI, *Il conferimento di Know-how*, cit., 18, in part. nt. 11.

Non è da credere che la rafforzata tutela dei segreti commerciali sia così decisiva nella scelta tra segreto e brevetto; gran parte delle valutazioni che si faranno in questa scelta sono le stesse di oggi⁸⁶. Cosicché, il brevetto sarà la scelta più oculata in presenza di segreti facilmente accessibili tramite *reverse engineering*⁸⁷, altrimenti correndo il rischio di un uso simultaneo del segreto o che nella misura in cui la commercializzazione del prodotto non costituisca predivulgazione il concorrente brevetti validamente l'invenzione, costringendo il (primo) detentore ad attenersi alle regole e ai limiti del preuso. Per contro, si opterà per il segreto quando esso non sia facilmente accessibile (si pensi ad una formula chimica o un segreto di procedimento) o sia alto il rischio di contraffazione dell'invenzione brevettata e non sostenibile, per i costi o altro motivo, la difesa del brevetto.

La rafforzata tutela dei segreti commerciali, di cui è segno evidente la responsabilità oggettiva del terzo, non fa poi del segreto commerciale un diritto dominicale pieno: il segreto non attribuisce, come poc'anzi visto, una privativa assoluta e la stessa tutela incontra molti e numerosi limiti esterni, non conciliabili con una concezione proprietaria.

Certo non si può negare che alcuni divieti di brevettazione per ragioni di liceità (ordine pubblico o buon costume) o perché implicano pratiche contrarie alla dignità ed integrità dell'uomo - si pensi ai divieti di esclusiva brevettuale del corpo umano o di sequenze isolate di geni o al divieto di utilizzazione di cellule

⁸⁶ Il *trade-off* tra segreto commerciale e brevetto per invenzione può così essere sintetizzato: (i) il brevetto ha una durata limitata nel tempo, ventennale, il segreto dura finché non vi è divulgazione o qualche concorrente non lo scopra in modo autonomo o venga decompilato; (ii) il segreto offre una tutela oggettiva più ampia, nel senso che esso riguarda anche informazioni non brevettabili; (iii) nell'esame della domanda di brevettazione, l'Ufficio non deve valutare il valore economico dell'invenzione, essendo questo irrilevante ai fini della brevettabilità, mentre per il segreto commerciale è richiesto che abbia un valore economico; (iv) il brevetto gode di una presunzione legale di validità, cui corrisponde in presenza di un brevetto di procedimento una presunzione di contraffazione rispetto ad ogni prodotto identico a quello ottenuto mediante il procedimento brevettato, salva la prova contraria (art 67 c.p.i.); diversamente per il segreto commerciale, ove l'onere di provare la violazione del segreto incombe sul legittimo detentore; (v) il costo per ottenere e mantenere un brevetto è sufficientemente determinabile. Quello di tutela di un segreto, lo è di meno perché comprende la spesa in misure di protezione, la cui adeguatezza impone un costante aggiornamento nel tempo, nonché i costi di transazione degli accordi di segretezza o patti di non concorrenza, non facilmente prevedibili; (vi) il brevetto è preferibile per motivi di *business*. Dopo il deposito di una domanda di brevettazione, l'inventore può fare affidamento su di essa. Può divulgare dettagli dell'invenzione a potenziali partner, investitori, acquirenti, poiché vi è un rischio minimo di contraffazione. Per contro, gli innovatori che si affidano alla segretezza devono utilizzare restrizioni contrattuali per garantire che la divulgazione non distrugga il valore dell'innovazione; (vii) infine, i brevetti sono più semplici da valutare rispetto ai segreti, e perciò il mercato può trattare i brevetti come un elemento del patrimonio aziendale.

⁸⁷ V., A. A. SCHWARTZ, *The Corporate Preference for Trade Secret* 74 Ohio St. L.J. 623, 639 (2013).

staminali embrionali⁸⁸ - possano spingere verso l'uso in regime di segretezza⁸⁹; né si può sottacere che queste problematiche hanno importanza e sempre più l'avranno nel futuro rispetto all'evoluzione della ricerca biotecnologica ispirata

⁸⁸ Nel caso *Brüstle* (Corte di giustizia, Grande sez., 18 ottobre 2011, C-34/10, Oliver Brüstle v. Greenpeace) la Corte definisce il concetto di embrione umano come ovulo umano fin dalla fecondazione ed esclude la brevettabilità di un'invenzione che richieda la previa distruzione di embrioni umani o la loro utilizzazione come materiale di partenza, indipendentemente dallo stadio in cui esse hanno luogo e anche qualora la descrizione dell'insegnamento tecnico oggetto di rivendicazione non menzioni l'utilizzazione di embrioni umani. Nella specie, il signor Brüstle è titolare di un brevetto tedesco su cellule staminali, isolate e purificate, precursori di neuroni, sui processi necessari per la loro produzione a partire da cellule staminali embrionali e sull'uso delle cellule precursori per il trattamento di patologie neuronali. Il brevetto è contestato da Greenpeace davanti al Tribunale Federale dei Brevetti della Germania che lo invalida. Il signor Brüstle decide di appellarsi alla Corte Federale di Giustizia della Germania, che solleva la questione pregiudiziale con alcune domande riguardanti l'interpretazione del termine «embrioni umani» presente nell'articolo 6(2)(c) della Direttiva 98/44/CE.

In dottrina, O. CAPASSO, *Gli sviluppi delle ricerche sulle staminali e la giurisprudenza in materia di brevetti biotecnologici*, in *Dir. ind.*, 2016, 140. Sulla nozione di embrione umano in senso ampio, A. TARANTINO, *Natura dell'uomo e modelli di biotica*, Milano, 2016, 19. Per un approccio critico alla sentenza della Corte di Giustizia, V. SGARAMELLA, *Non più cose, non ancora persone. Gli embrioni tra brevetti e funerali*, in *il Mulino*, 2012, 280.

⁸⁹ Nel caso *Myriad Genetics (Ass'n for Molecular Pathology v. Myriad Genetics, Inc.)*, 133 S. Ct. 2107, 2120 (2013), la corte invalida le rivendicazioni di un brevetto detenuto dalla società di biotecnologia Myriad Genetics, che riguardava sequenze di DNA, i geni BRCA1 e BRCA2 denominati *geni del cancro della mammella* perché le loro mutazioni sono correlate con un aumento del rischio di cancro al seno (e del cancro ovarico). I tumori al seno derivanti da mutazioni in questi geni rappresentano tra il 5% e il 10% di tutti i tumori al seno. Il rischio del cancro ovarico è di circa il 55%, per le donne con mutazioni BRCA1 e circa il 25%, per le donne con mutazioni BRCA2. In qualità di titolare dei brevetti sui geni BRCA1 e BRCA2, Myriad Genetics commercializza il test di screening diagnostico per le mutazioni genetiche, ciò che gli conferisce un monopolio su tutti i test BRCA1/2 negli Stati Uniti (\$ 3000 per test), impendendo di sviluppare test di screening alternativi. L'*American Civil Liberties Union* contesta la validità di questo brevetto e la corte dichiara che le sequenze rivendicate non sono brevettabili in quanto *products of Nature* (35 U.S.C. § 101). Ma prima che il caso fosse deciso, Myriad cambia strategia: forma un database segreto di mutazioni genetiche e delle malattie associate che continua a commercializzare in regime di segretezza.

Per una lettura critica della sentenza, in quanto avrebbe mancato di affrontare il tema della brevettabilità sotto il profilo della violazione, di quello che da noi si direbbe, dell'ordine pubblico e del buon costume, L. G. ELI, *When Myriad Genetics prohibited a myriad of options: Association For Molecular Pathology v. USPTO* 21 DePaul J. Art Tech. & Intell. Prop. L. 357 (2011). V., anche, G. CONTALDI, *Considerazioni di diritto internazionale sul caso Myriad Genetics*, in E. Arezzo, F. Falce, G. Olivieri (a cura di), *Confini e fronte dell'innovazione biotecnologica per la proprietà intellettuale*, Milano, 2014, 43, ove, a nt. 4, ampi riferimenti bibliografici sul caso. L'A. esclude che l'Accordo TRIPs faccia obbligo agli Stati membri di rilasciare il brevetto per le mere decodifiche di frammenti di DNA e ciò sulla base di una lettura funzionale, sull'assunto che l'isolamento del DNA non presenta i caratteri della scoperta (58) e che difettano altresì i requisiti dell'attività inventiva e di industrialità (59).

al c.d. transumanesimo⁹⁰, e a cui si associano rischi di eugenetica⁹¹ e che pone domande sul futuro stesso dell'umanità. In tal caso, però, bisognerà pur affermare, per un elementare principio di unità e coerenza dell'ordinamento, che non è consentito tutelare come segreti commerciali quelle invenzioni che il legislatore vieta di brevettare, la cui attuazione è contraria all'ordine pubblico o al buon costume.

⁹⁰ Gli obiettivi del movimento transumanista sono riassunti da M. O'CONNEL, *To Be a Machine: Adventures among Cyborgs, Utopians, Hackers, and the Futurists Solving the Modest Problem of Death*, Trade Paperback, Demy PB, 2017: si tratta della tesi dell'integrazione dell'uomo con la macchina (ad es. il cervello con un processore elettronico), non per colmare un deficit fisico o curare qualche disfunzione, bensì per aumentare le capacità dell'uomo oltre il naturale, e raggiungere l'obiettivo ultimo dell'immortalità. V, anche, R. MCKIE, *No death and an enhanced life: Is the future transhuman?*, in *The Observer*, 6 maggio 2018.

⁹¹ L. C. IKEMOTO, *Race to Health: Racialized Discourses in a Transhuman World* 9 DePaul J. Health Care L. 1101 (2005).