

IL “DATO”: BENE IMMATERIALE CON UN PROPRIO VALORE INTRINSECO

Manlio d’Agostino Panebianco

BASC Università Milano Bicocca

ABSTRACT [ENG]: *Data and information characterize the modern globalized society, becoming one of the main value-added assets. Indeed, the use of the most advanced technologies (in particular, Artificial Intelligence) has made their role strategic in the chain for the creation of economic value, while generating new risks, both of a social and managerial nature. Jurisprudence has already deduced some effects, expressing very interesting positions that go beyond the mere legal context, and flowing into the economic one, requiring serious reflection, inter alia, for a revision of the financial reporting models to stakeholders.*

ABSTRACT [ITA]: Il dato e l’informazione caratterizzano la moderna società globalizzata, divenendo uno tra i principali beni a valore aggiunto. Invero, l’impiego delle più evolute tecnologie (in particolare l’Artificial Intelligence) ha reso strategico il loro ruolo nella catena per la creazione del valore economico, pur ingenerando nuovi rischi, tanto di carattere sociale, quanto gestionale. La giurisprudenza ha già rilevato alcuni effetti, esprimendo posizioni molto interessanti che travalicano il mero contesto legale, e sfociando in quello economico, impongono una seria riflessione, *inter alia*, per una revisione dei modelli di rendicontazione agli *stakeholders*.

KEYWORDS: bene immateriale, patrimonializzazione, valore aggiunto, artificial intelligence, privacy

SOMMARIO: 1. Introduzione. - 2. Informazioni, dati, dati personali e *files*. - 3. I dati come “beni immateriali”. - 4. Gli illeciti ed i reati nella “dimensione digitale”. - 5. Il rapporto tra IP, capitale umano ed i dati. - 6. Una considerazione conclusiva su due rischi derivanti.

1. Introduzione.

La Globalizzazione è un fenomeno antico, che può essere ricondotto all’innato desiderio di scoprire, di esplorare e di viaggiare, ampliando i propri orizzonti, conoscenze e, non ultimo obiettivi. Nei millenni, questa ha assunto forme diverse, ed i suoi confini erano fortemente influenzati dalle possibilità “tecniche” e culturali. Basti pensare ai grandi imperi del passato (da quello Mongolo a quello Romano) che avevano una estensione molto rilevante, proprio in relazione alla capacità di spostamento. In quel contesto, è anche significativo l’impatto culturale, che spesso limitava quel desiderio di “andare oltre”: basti richiamare alla memoria, le cosiddette “*colonne d’Ercole*”, che nella cultura classica,

individuavano quel limite estremo del mondo conosciuto, che non si poteva e (soprattutto) non si doveva superare. Eppure, grandi viaggiatori, navigatori ed esploratori (i più noti sono Marco Polo, Cristoforo Colombo, Vasco da Gama, Albuquerque, Abreu e Serrão, Vasco Núñez de Balboa, solo per citarne alcuni) hanno dimostrato come alcuni limiti fossero solo legati alla conoscenza del momento.

Se proprio le “*colonne d’Ercole*” definiscono metaforicamente il concetto di “limite della conoscenza”, d’altro canto Giovenale, nelle Satire, citava «*rara avis in terris nigroque simillima cygno*», per indicare la quasi impossibilità che un cigno possa essere di un colore diverso dal bianco. Altra circostanza smentita dagli esploratori europei che, nel 1697, sbarcando nell’odierna Australia videro con i propri occhi il “*Chenopsis atrata*”, ossia il cigno nero.

In questo contesto, molti secoli dopo, Nassim Nicholas Taleb¹, uno scrittore e statistico libanese-americano, elaborò la sua “*Black Swan theory*”² per descrivere come la “presunzione” (ossia non conoscenza completa, in taluni casi completa ignoranza) su determinati eventi, circostanze, fatti, porti ad escludere le possibili (e spesso, significative) opzioni alternative, ponendole ai margini delle aspettative umane, storiche, scientifiche, economiche e tecnologiche³.

Ma cosa c’entra tutto ciò con la moderna società, i dati e le informazioni?

Semplicemente, l’attuale Globalizzazione è il risultato di un avanzato progresso tecnologico nel settore delle telecomunicazioni e dei trasporti, che abbattendo le barriere fisiche, geografiche e temporali, ha messo in relazione in “tempo reale” gli angoli più remoti del nostro pianeta. Il cuore di questo fenomeno sociale ed economico, è da ricondursi alla capacità della ICT⁴ di rendere disponibili informazioni e dati, in grande quantità ed a velocità mai prima d’ora ipotizzabili, a qualunque persona.

Se, dunque, è pensabile che dopo il fenomeno della Globalizzazione ne seguirà un altro⁵, è altrettanto vero che questa materia riguarda, direttamente ed indirettamente, il “*capitale umano*” ossia l’insieme di tutte le capacità cognitive derivanti dal patrimonio di conoscenze, competenze e abilità tecniche⁶, di cui ciascuna persona si arricchisce nel corso della propria vita, utilizzandole come “strumenti a valore aggiunto” per ogni attività svolta, e che viene consegnato alle generazioni successive, attraverso un processo naturale tramandamento.

Anche in questo caso, il contenuto trasferito avviene per il tramite di elementi (ossia, i dati e le informazioni), talmente comuni e di uso frequente, che raramente ci si sofferma a pensare sulla loro definizione e perimetro.

2. Informazioni, dati, dati personali e files.

L’introduzione vuole puntare a stimolare l’attenzione e l’interesse sul significato e sul valore di ciascuno di questi elementi, soprattutto gettando le basi per la comprensione di

1 N. N. TALEB, *The Black Swan: The Impact of the Highly Improbable*, Penguin Books, 2008

2 Sebbene in letteratura venga più appropriatamente definita come *metafora*, *paradigma* o *logica*.

3 Per un approfondimento sul tema in ambito giuridico, si consiglia A. SPINOSA, *Il cigno nero*. *Diritti, potere e libertà di fronte al silenzio della legge. Un dibattito teorico di primo novecento*, in *Historia et Ius*, 2020, n.18.

4 Acronimo di *Information and Communication Technology*.

5 L’essere umano, forse, un giorno arriverà al tanto agognato concetto di “universalizzazione”.

6 Si veda I. VISCO, *Capitale umano e crescita (Intervento del Governatore della Banca d’Italia)*, Università Cattolica del Sacro Cuore, 30 gennaio 2015.

quello che il dinamico processo evolutivo che li caratterizza, sia dal punto di vista tecnologico, ma anche e soprattutto sociale, economico e giuridico⁷.

La prima considerazione che deve necessariamente essere fatta, è che troppo spesso l'uso comune di associa al medesimo significato, mentre sono significative le differenze.

Infatti, consapevoli della tridimensionalità della vita⁸, possiamo definire il dato come un qualunque "elemento" espresso in forma di numero, testo, immagine, video, audio, etc. che può essere riprodotto e memorizzato con formati diversi (tanto digitali, quanto materiali), e che sebbene abbia un "valore proprio", può assumere significati differenti in ragione alla sua contestualizzazione.

D'altro canto, l'informazione è un dato spesso elaborato, di certo inserito in un contesto specifico, alla quale si può attribuire un puntuale e chiaro significato.

Sembra opportuno notare come in letteratura, l'informazione viene anche descritta «*come "un messaggio comunicabile ad altri attraverso un mezzo qualsiasi": essa può quindi essere oggetto di rapporti giuridici ed in particolari contrattuali ed in queste ipotesi assume un valore economico per chi la "detiene", sia esso un soggetto privato oppure pubblico. L'informazione è in generale un bene immateriale per cui per essa non è replicabile la scarsità che esiste in natura per quelli fisici; quindi la sua utilizzazione da parte di un soggetto non esclude che anche un altro la possa contemporaneamente sfruttare (cd. non rivalità e possibilità di "un godimento plurimo e solidale")*»⁹.

In questo senso, però, è opportuno evidenziare come l'evoluzione etimologica degli ultimi decenni, abbia fatto emergere altri due termini, ai quali possono essere associati significati simili e spesso fuorvianti.

Il primo riguarda i Big-Data, per il quale non esiste - in letteratura e nella comunità scientifica - una unica definizione scientifica condivisa, pur tuttavia potendo individuare almeno 4 elementi caratterizzanti:

- a) il grande volume di dati;
- b) l'ampia varietà di formati, fonti e tipi;
- c) l'elevata velocità di ricerca e reperimento dati;
- d) la veridicità e coerenza delle conclusioni basate sui dati.

Sono, quindi, grandi masse di "semplici dati" od anche l'insieme di "tutti i dati" che quotidianamente vengono generati, elaborati ed immessi in tutto il sistema digitale (quindi, sia nella "rete", sia nei singoli server), che si stratificano non sempre in modo ordinato ed utilizzabile, e difficilmente possono essere utilizzati se non grazie all'impiego di complesse strutture software, più avanzate rispetto nelle logiche rispetto ai modelli classici. Pertanto, in coerenza con alcuni autori, la "eccessiva" dimensione (caratteristica intrinseca) diventa tanto un punto di forza, quanto potenzialmente un limite. Ad esempio, richiamando T.H.

⁷ Si presti attenzione che i citati ambiti sono interconnessi tra loro, e non possono in alcun modo essere considerati come autonomi.

⁸ Si fa riferimento alle 3 dimensioni (reale, digitale e virtuale) su cui ciascuna persona, oggigiorno, si esprime e relazione nel contesto sociale. In tal senso, si veda, M. D'AGOSTINO PANEBIANCO, *Vivere nella Dimensione Digitale*, Themis ed., 2019. D'altro canto, Floridi individua nella "infosfera" quello spazio che *de facto* ricomprende la dimensione reale e quella digitale, senza soluzione di continuità alcuna tra le due: si veda L. FLORIDI, *Pensare l'infosfera, la filosofia come design concettuale*, Raffaello Cortina Ed., 2020.

⁹ A.M. ROVATI, *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici*, in *Rivista Informatica e diritto*, Vol. XX, 2011, n. 1-2, p.155.

Davenport i «*Big Data si riferiscono a dati che sono troppo grandi per entrare in un singolo server e troppo non strutturati per entrare in una tabella di righe e colonne*»¹⁰.

In tal senso, d'altro canto, l'evoluzione dell'*Artificial Intelligence* e delle tecniche di *Machine Learning* (che si è sviluppata parallelamente a quella dell'ICT, con sempre più frequenti interazioni) ha innescato un processo di utilizzo a "valore aggiunto" dei Big-Data, dando vita ai cosiddetti "Smart Data" (il secondo termine di interesse).

In effetti, gli Smart-Data sono il risultato di un accurato e complesso processo di selezione ed elaborazione "su misura" dei Big Data, con l'obiettivo di risolvere specifiche problematiche e/o per il raggiungimento di obiettivi fissati dal "soggetto decisore", e (come avviene per le *informazioni*) in relazione ad uno specifico contesto.

È, però, necessario ed opportuno fare una doverosa chiosa in merito: l'*Artificial Intelligence* ed i suoi "prodotti" devono comunque rispondere al primario principio di essere al servizio della persona umana¹¹, nel pieno e costante rispetto dei diritti e delle libertà fondamentali¹², e non finalizzate a generare profitto economico a tutti i costi, secondo un diffuso *utilitarismo*¹³. «*Ciò comporta che il fine primario non sarebbe quello di costruire macchine che sostituiscano le persone, ma sistemi che amplifichino e aumentino le capacità dell'essere umano, facendo interagire intelligenza artificiale e persone al fine di risolvere fenomeni e problemi complessi*»¹⁴.

10 Si veda G. ARBIA, *Statistica, nuovo empirismo e società nell'era dei Big Data*, Nuova Cultura Ed., 2018, p.43.

11 In tal senso, sembra calzante ricordare l'affermazione di Gesù riportata, sia nel Vangelo di Marco (Mc 2,27) che di Luca (Lc 14,1-6), che «*il sabato è stato fatto per l'uomo e non l'uomo per il sabato*».

12 In tal senso, sembra opportuno richiamare PAPA BENEDETTO XVI, *Lettera Enciclica Caritas In Veritate*, Vaticano, 29 giugno 2009, n.70: «*Lo sviluppo tecnologico può indurre l'idea dell'autosufficienza della tecnica stessa quando l'uomo, interrogandosi solo sul come, non considera i tanti perché dai quali è spinto ad agire. È per questo che la tecnica assume un volto ambiguo. Nata dalla creatività umana quale strumento della libertà della persona, essa può essere intesa come elemento di libertà assoluta, quella libertà che vuole prescindere dai limiti che le cose portano in sé. Il processo di globalizzazione potrebbe sostituire le ideologie con la tecnica, divenuta essa stessa un potere ideologico, che esporrebbe l'umanità al rischio di trovarsi rinchiusa dentro un a priori dal quale non potrebbe uscire per incontrare l'essere e la verità. In tal caso, noi tutti conosceremmo, valuteremmo e decideremmo le situazioni della nostra vita dall'interno di un orizzonte culturale tecnocratico, a cui apparterremmo strutturalmente, senza mai poter trovare un senso che non sia da noi prodotto. Questa visione rende oggi così forte la mentalità tecnicistica da far coincidere il vero con il fattibile. Ma quando l'unico criterio della verità è l'efficienza e l'utilità, lo sviluppo viene automaticamente negato. Infatti, il vero sviluppo non consiste primariamente nel fare. Chiave dello sviluppo è un'intelligenza in grado di pensare la tecnica e di cogliere il senso pienamente umano del fare dell'uomo, nell'orizzonte di senso della persona presa nella globalità del suo essere. Anche quando opera mediante un satellite o un impulso elettronico a distanza, il suo agire rimane sempre umano, espressione di libertà responsabile. La tecnica attrae fortemente l'uomo, perché lo sottrae alle limitazioni fisiche e ne allarga l'orizzonte. Ma la libertà umana è propriamente se stessa solo quando risponde al fascino della tecnica con decisioni che siano frutto di responsabilità morale. Di qui, l'urgenza di una formazione alla responsabilità etica nell'uso della tecnica. A partire dal fascino che la tecnica esercita sull'essere umano, si deve recuperare il senso vero della libertà, che non consiste nell'ebbrezza di una totale autonomia, ma nella risposta all'appello dell'essere, a cominciare dall'essere che siamo noi stessi*».

13 La critica, condivisa da molte scuole di pensiero, è che non sempre la massimizzazione del "benessere individuale" conduce al "benessere della collettività", dovendo prestare attenzione ai possibili conflitti tra la naturale propensione dell'agire utilitaristico del singolo individuo per ricercare la propria massima utilità (*act utilitarianism*), ed il ruolo del pubblico di perseguire il massimo benessere sociale (*rule utilitarianism*), anche attraverso l'introduzione di misure correttive.

14 G. ZICCARDI, *Legal Tech Books (S01 E03) Francesca Rossi, "Il confine del futuro"*, 2020

Questo è tanto vero nella sua prospettiva generale, quanto ancora più significativo quando si affronta la tematica della protezione dei dati personali (ossia una specifica categoria riferibile alla “persona umana”¹⁵), allo stato normata dal Regolamento (UE) 2016/679¹⁶. Infatti, il Regolamento introduce una serie di principi e di innovazioni. *In primis*, sancisce che “la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale”¹⁷ ponendo al centro una questione di natura etica, prima che “regolamentare”. Quindi, modifica l’approccio giurisdizionale, poiché è applicabile (a) sia quando il trattamento di dati personali viene effettuato da parte di un Titolare¹⁸ o di un Responsabile¹⁹ residenti in un Paese dello Spazio SEE²⁰, indipendentemente che questo venga effettuato o meno all’interno dello stesso; (b) sia quando il trattamento dei dati riguardi degli “interessati”²¹ che si trovano nell’Unione effettuato, da parte di un titolare del trattamento o da un responsabile del trattamento non stabilito nell’Unione, e quando le attività di trattamento sono connesse all’offerta di beni o servizi a detti interessati (indipendentemente dal fatto che vi sia un pagamento correlato)²².

In questo modo, il legislatore Europeo ha modificato *de facto* il tradizionale approccio, andando a tutelare i diritti e le libertà fondamentali dei cittadini europei, anche oltre i confini geografici dei Paesi membri.

Tutto ciò premesso, il GDPR fornisce una prima specifica definizione di una particolare categoria di dati (che come vedremo in seguito, ha delle conseguenti declinazioni), che riguarda il “dato personale”: questo è «qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»²³.

Come detto, e come si evince chiaramente dalla precedente, il Legislatore Europeo ha inteso fornire anche una serie di puntuali declinazioni, alle quali corrispondono altrettanto specifiche indicazioni e limitazioni di trattamento: infatti, le caratteristiche di alcune “sotto-categorie” sono particolarmente “sensibili”, potendo esporre l’interessato ad una serie di

15 Qui intesa con l’accezione e la dignità che ha voluto dare l’art.3 della Costituzione Italiana.

16 Meglio conosciuto come *GDPR* (dall’inglese *General Data Protection Regulation*).

17 Considerando 1) Regolamento (UE) 2016/679.

18 Cfr. Regolamento (UE) 2016/679, art.4 punto 7).

19 Cfr. Regolamento (UE) 2016/679, art.4 punto 8).

20 Lo Spazio Economico Europeo (SEE) è stato istituito nel 1994 allo scopo di estendere le disposizioni applicate dall’Unione europea al proprio mercato interno ai paesi dell’Associazione europea di libero scambio (EFTA). Pertanto, il GDPR è vigente in tutti i Paesi dell’Unione Europea, ed anche alla Norvegia, l’Islanda e il Liechtenstein (che sono membri del SEE), ma non la Svizzera (che sebbene faccia parte dell’EFTA, non rientra nel SEE).

21 A differenza della precedente legislazione italiana (Decreto legislativo 30 giugno 2003, n. 196 all’articolo 4. co.1 lettera i) in cui l’interessato veniva espressamente definito come «la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali», nel Regolamento UE n.679/2016, questa è desumibile il suo significato prevalentemente da quella di “dato personale” (cfr. Articolo 4, punto 1) quando viene correlata “qualsiasi informazione” ad “una persona fisica identificata o identificabile”.

22 Cfr. Considerando 23-26 del Regolamento (UE) 2016/679.

23 Rubricata all’art.4 co.1 del Regolamento (UE) 2016/679.

rischi circa la violazione della propria dignità, l'esercizio dei propri diritti o manifestazione delle proprie libertà.

È il caso dei *"dati particolari"*²⁴, che riguardano quei dati personali *«che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale»* ovvero i dati genetici²⁵, biometrici²⁶, e relativi alla salute²⁷ o alla vita sessuale o all'orientamento sessuale della persona. È opportuno rilevare come, quantomeno in Italia, vi sia una sostanziale continuità logica (benché, ampliata nella portata) con la precedente definizione di "dato sensibile" data dal "Codice in materia di protezione dei dati personali"²⁸.

Orbene, a questo punto, si appalesa un aspetto pratico: i dati e le informazioni sono elementi, ma dove sono "contenuti" (ossia registrati)?

Se nella dimensione *reale*, questi possono riguardare (quantomeno, principalmente) la carta sui cui possono essere stampati o trasposti (ad esempio, in modo olografo o olografico) con le diverse tecniche, nella dimensione *digitale* è necessario fare riferimento al "contenitore" per antonomasia, ossia il "file".

Ancora una volta, è opportuno adottare una metodologia etimologica per meglio circoscrivere il perimetro: il termine inglese "file" ha origine latina (*filum*), assumendo un significato più tradizionale di fascicolo²⁹ (od anche, archivio), mentre nel moderno uso comune, correlato alla sfera digitale, è quella sorgente che si può leggere e scrivere, ovvero quel contenitore immateriale di informazioni e dati, logicamente correlati, che sono memorizzati e conservati in un supporto fisico, elaborabile solo attraverso un apposito software predisposto a quella specifica operazione.

3. I dati come "beni immateriali".

È evidente come, ormai, i dati abbiano un proprio valore ed esista una diretta correlazione e collegamento tra i "beni intangibili" (supporto) ed il "dato".

In effetti, questa nuova posizione ha aperto - proprio nel corso degli ultimi anni - a nuove interessanti interpretazioni tanto dottrinali, quanto giurisprudenziali su cui sembra opportuno potersi soffermare, proprio in materia di "beni intangibili" e rispetto alla

24 La cui definizione è rubricata all'art. 9 del Regolamento (UE) 2016/679.

25 Nel Regolamento (UE) 2016/679 all'art.4 co.13) per "dati genetici" si intendono: *«i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione».*

26 Nel Regolamento (UE) 2016/679 all'art.4 co.14) per "dati biometrici" si intendono: *«i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».*

27 Nel Regolamento (UE) 2016/679 all'art.4 co. 15) per "dati relativi alla salute" si intendono: *«i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».*

28 Infatti, il Decreto Legislativo 30 giugno 2003, n. 196 all'articolo 4 co. 1 lettera d), definisce i "dati sensibili" quali *«i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».*

29 Questo è caratteristico della dimensione reale, e del linguaggio amministrativo e burocratico.

definizione di “cosa mobile”, ma anche e soprattutto agli effetti derivanti, tanto giuridici quanto economici.

In primis, è opportuno evidenziare come «data la natura complessa dei beni intangibili non esiste una definizione universalmente condivisa né un metodo unico per misurarli (Corrado, Hulthen and Sichel, 2005; CHS). La letteratura identifica quindi tre caratteristiche fondamentali per classificare un bene come intangibile: 1) è una fonte probabile di profitto futuro; 2) non è identificabile con parametri fisici; 3) può essere usato come merce di scambio dalle imprese (OCSE, 2008)»³⁰.

Questa argomentazione deve essere letta alla luce di una attenta osservazione delle modalità di creazione di valore, in particolar modo dei *Big Tech Giant*: questi, infatti, implementano sempre nuove applicazioni³¹ disponibili “gratuitamente” online, con l’intento di raccogliere ed elaborare dati (ovvero, avviare sempre più raffinati ed attendibili meccanismi di *profilazione*³²). È, però, necessario prestare attenzione che la gratuità di questo processo è solo apparente, poiché genera un profitto economico-finanziario (una vera e propria entrata ben individuabile nei bilanci aziendali), basato sull’acquisizione di dati (anche di natura personale, comportamentale, etc.), in forza di un consenso rilasciato, molto spesso in modo non sempre totalmente consapevole.

Infatti, è opportuno ricordare che «il “dato personale” è assimilabile ad un “bene” che ha un proprio valore intrinseco, ed è innegabile come nel nuovo contesto digitale i dati siano diventati la fonte principale di creazione di valore»³³.

Tale affermazione, non è solo frutto di una critica di buon senso, ma è riscontrabile anche nelle considerazioni³⁴ alla base della Direttiva (UE) 2019/770 del Parlamento Europeo e del Consiglio del 20 maggio 2019: il Legislatore Europeo, proprio con riferimento a quei contratti di fornitura di contenuto digitale e di servizi digitali, richiama espressamente il caso in cui quando a fronte di una fornitura di contenuti o servizi digitali, non vi sia una controprestazione in denaro, ma si effettui un “pagamento” con il conferimento di dati personali.

Nello spirito di non limitare le “naturali” evoluzioni del mercato, bensì di limitare quegli eccessi che potrebbero minare l’esercizio di propri diritti e libertà (in specie, quando fondamentali), tale statuizione viene ridimensionata³⁵ nella medesima Direttiva, quando

30 C. JONA-LASINIO, *Il capitale immateriale e i territori italiani*, in AA.VV., *5° Rapporto sulla classe dirigente*, Rubettino Editore, 2011, p. 133.

31 Si fa riferimento, in particolare, ai cosiddetti *On-Line Social Networks*, che raccolgono dati ed abitudini di comportamento e consumo, con la finalità di commercializzarli per supportare i processi di *e-marketing*, per rendere le offerte rivolte ai clienti (effettivi o potenziali), sempre più aderenti e personalizzate quantomeno nella percezione. Ovviamente, questa metodologia è evidentemente una tecnica di persuasione sempre più efficace (molto spesso al limite con il rispetto della libertà di scelta individuale), che è alla base persino della nuova figura dell’influencer.

32 Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) all’articolo 4 co.4 definisce la *profilazione* come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica».

33 Cfr. M. D’AGOSTINO PANEBIANCO, *op.cit.*, p.116.

34 si veda il Considerando 24, successivamente declinato, ad esempio, all’art.3.

35 fortunatamente e condivisibilmente.

expressis verbis chiarisce che «*tali dati non possono dunque essere considerati una merce*» ed anzi lo spirito della direttiva dovrebbe essere teso a garantire «*che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali*», richiamando espressamente le disposizioni vigenti in materia di protezione dei dati personali (leggasi, Regolamento UE 2016/679), ed i principi di liceità e finalità.

Sin qui, possiamo dire che siamo giunti alla conclusione che il dato è stato al centro di un processo di patrimonializzazione, che lo rende a “valore intrinseco” o a “valore aggiunto”, riportando per analogia alla sfera dei beni intangibili.

Il quadro si arricchisce e completa con alcune posizioni della giurisprudenza italiana, chiarendo in modo (quantomeno, apparente) il nuovo perimetro in cui ci si muove.

La (cosiddetta) “*patrimonializzazione*” del dato personale³⁶, infatti, è già stata oggetto di pronunce da parte di alcune Corti: la pietra miliare è certamente individuabile nella sentenza della Corte di Cassazione Sez. II, 7 novembre 2019 (dep. 10 aprile 2020), n. 11959, che introduce una innovativa interpretazione giurisprudenziale, chiarendo come il *dato informatico* possieda un indiscusso valore patrimoniale, in ragione delle facoltà di utilizzazione e del contenuto specifico del singolo dato³⁷.

La questione affrontata nella sentenza riguarda un procedimento per appropriazione indebita, in cui afferma come i *file* sono riconducibili al concetto di “*cosa mobile*”, ed attraverso un articolato percorso interpretativo, identifica la cosa mobile con un'entità fisica suscettibile di essere materialmente appresa, ossia una entità materiale idonea a soddisfare un bisogno umano [purché si tratti di] una parte del mondo esterno, avente una *dimensione fisica*, che possa essere trasportata da un luogo all'altro e sottratta al legittimo possessore.

Infatti, la Cassazione, osserva che «*quanto alla fisicità “in senso stretto” [...] il file è un supporto sul quale vengono immagazzinati i dati, che occupa uno spazio misurabile in bit e che può essere trasferito da un dispositivo a un altro, anche utilizzando la rete internet; si tratterebbe, quindi, di un'entità fisica, ancorché non percepibile attraverso i sensi*»³⁸. In tal senso, la Cassazione argomenta che «*tra i presupposti che la tradizione giuridica riconosce come necessari per ravvisare le*

36 Come effetto derivante dall'ottenimento di un servizio digitale, in specie nell'ambito delle attività dei “social network”, che a fronte del conferimento dei propri dati personali, utilizzabili ai fini di *profilazione* e commercializzazione in favore di terzi.

37 A. DI TULLIO D'ELISIIS, *I dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale*, in *Diritto&Diritti*, 2020

38 Cfr. C. PAGELLA, *La Cassazione sulla riconducibilità dei file al concetto di “cosa mobile” oggetto di appropriazione indebita: un caso di analogia in malam partem?*, in *Sistema Penale*, 2021. D'altronde, non tanto dal punto di vista penale in relazione al reato di appropriazione indebita, bensì proprio nella prospettiva di classificare i *files* ed i dati (tanto informatici quanto personali) nella sfera dei beni, anche di natura patrimoniale, risulta utile richiamare (nonostante le perplessità che manifesta) anche N. PISANI, *La nozione di “cosa mobile” agli effetti penali e i 'files' informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in *Diritto penale e processo*, 5/2020, pp. 651-655: «*I dati informatici ('files') sono qualificabili come cose mobili ai sensi della legge penale e sono, quindi, suscettibili di appropriazione rilevante ai sensi dell'art. 646 c.p. laddove sottratti da un 'personal computer' aziendale e successivamente cancellati dallo stesso. È quanto affermato dalla Corte di cassazione che nell'assumere a criterio di sussumibilità la dimensione offensiva della condotta, ritiene sia consentita una ricostruzione della nozione di cosa mobile alla stregua dell'evoluzione dei referenti linguistici. Tuttavia, tale ricostruzione presta il fianco a seri dubbi di compatibilità con il principio di tassatività della legge penale, rischiando di trasformare il tipo legale “astratto” in fattispecie a forma libera di evento*».

condotte di sottrazione e impossessamento (o appropriazione) di cose mobili, il criterio della necessaria detenzione fisica della cosa è quello che desta maggiori perplessità. Se la ratio, sottesa alla selezione delle classi di beni suscettibili di formare oggetto delle condotte di reato di aggressione all'altrui patrimonio, è agevolmente individuabile nella prospettiva della correlazione delle condotte penalmente rilevanti (essenzialmente, quelle che mirano alla sottrazione della disponibilità di beni ai soggetti che siano titolari dei diritti di proprietà o di possesso sulle cose considerate) all'attività diretta a spogliare il titolare del bene dalla possibilità di esercitare i diritti connessi all'utilizzazione del bene, è chiaro che la sottrazione (violenta o mediante attività fraudolenta o, comunque, dirette ad abusare della cooperazione della vittima) debba presupporre in via logica la disponibilità, da parte dei soggetti titolari, dei beni su cui cade la condotta penalmente rilevante; ma anche in questo contesto deve prendersi atto che il mutato panorama delle attività che l'uomo è in grado di svolgere mediante le apparecchiature informatiche determina la necessità di considerare in modo più appropriato i criteri classificatori utilizzati per la definizione di nozioni che non possono rimanere immutabili nel tempo.

In questa prospettiva, dunque, si è giunti da parte delle più accorte opinioni dottrinali - in modo coerente con la struttura dei fatti tipici considerati dall'ordinamento (caratterizzati dall'elemento della sottrazione e dal successivo impossessamento) e dei beni giuridici che l'ordinamento intende tutelare sanzionando le condotte contemplate nel titolo XIII del codice penale - a rilevare che l'elemento della materialità e della tangibilità ad essa collegata, della quale l'entità digitale è sprovvista, perde notevolmente peso: il dato può essere oggetto di diritti penalmente tutelati e possiede tutti i requisiti della mobilità della cosa».

In effetti, è opportuno notare come la Suprema Corte in questa sentenza, richiami «l'orientamento della Corte costituzionale (espresso dalla sentenza 327 del 2008 e recentemente ribadito, tra le altre da C. cost. 141 e 278 del 2019, in materia di favoreggiamento della prostituzione) secondo il quale l'utilizzo di «espressioni sommarie, di vocaboli polisemi, ovvero di clausole generali o concetti elastici» non comporta la violazione del principio di precisione ogniqualvolta il giudice sia comunque in grado di «esprimere un giudizio di corrispondenza della fattispecie concreta alla fattispecie astratta, sorretto da un fondamento ermeneutico controllabile; e, correlativamente, permetta al destinatario della norma di avere una percezione sufficientemente chiara ed immediata del relativo valore precettivo»³⁹.

Risulta evidente, pertanto, come anche nell'ambito del trattamento del dato personale, il diritto tuteli sia la sfera personale⁴⁰, che il conseguente e relativo valore economico-patrimoniale derivante. Ma anche, che l'orientamento e l'evoluzione del diritto, vanno verso una posizione in cui una eventuale condotta di furto (e/o appropriazione indebita) di uno o più files - rientrando nel novero delle cose mobili - configuri nuovi ed interessanti scenari nell'ambito dei reati economici e di quelli della proprietà intellettuale, con chiari e possibili riferimenti anche al perimetro normativo del Decreto Legislativo 08/06/2001 n. 231. infatti,

³⁹ Cfr. C. PAGELLA, *op. cit.*

⁴⁰ Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) al Considerando (1) afferma che «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (Carta) e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE) stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano» ed all'articolo 1 co. 2 recita «Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali».

osservando le famiglie di reato rubricate al catalogo, è altresì opportuno, considerare che l'appropriazione indebita di un file, presuppone (quantomeno, ipoteticamente) anche il possesso e quindi un possibile trattamento⁴¹ illecito e/o non autorizzato di dati personali, ovvero di informazioni che potrebbero essere coperte dal segreto industriale o di altra natura.

4. Gli illeciti ed i reati nella “dimensione digitale”.

La nostra società è caratterizzata da una cultura “*data driven*”, ossia in cui i dati (anche considerati come rappresentazione oggettiva della realtà) sono l'elemento fondamentale su cui tutte le decisioni sono prese, lasciando meno spazio alle sensazioni umane e personali.

Se da un lato, tale affermazione tende ad aumentare l'efficienza, dall'altro una tal cultura potrebbe ingenerare delle distorsioni e dei circoli viziosi, legati alla frenetica ricerca di ottenere dati ed informazioni, non sempre in modo lecito. Il rischio, infatti, non solo non è remoto, ma stiamo assistendo ad un mutamento dei fenomeni illeciti e criminali, in funzione di obiettivi personali ed aziendali.

Risulta evidente come questa cultura influenzi fortemente il comportamento della singola persona, sia nella sottovalutazione di alcune cautele o modalità che dovrebbero essere adottate (con l'effetto di configurare una responsabilità colposa oppure negligenza, imprudenza o imperizia) piuttosto che nella configurazione di vere e proprie condotte penalmente rilevanti di natura dolosa⁴². Inoltre, in particolar modo in questo ambito, ciascun delitto potrebbe essere propedeutico alla commissione di un altro, integrandolo e divenendone “reato presupposto” (*predicate crimes*)⁴³.

Ad esempio, prendendo spunto dalla già citata sentenza della Corte di Cassazione Sez. II, 7 novembre 2019 (dep. 10 aprile 2020), n. 11959, che riconosce la possibilità di commettere il reato di appropriazione indebita di file⁴⁴, non è interessante solo per via dell'argomentazione circa l'immaterialità del bene (in quanto cosa mobile), ma sarebbe piuttosto interessante comprendere la finalità ultima del reo, ossia andrebbe letta in funzione dell'utilizzo che lo stesso vuole fare dei dati contenuti.

In effetti, come in un ragionamento ampio e più generale, salvo che l'atto dello spossessamento possa cagionare un danno, non sarebbe logico adottare una tale condotta fine a sé stessa: pertanto, per ipotesi, l'autore del reato potrebbe agire in tal senso, con l'obiettivo di utilizzare i “dati” contenuti in esso. Da cui, *in primis*, nasce l'esigenza di

41 In tal senso è necessario richiamare la definizione completa di “trattamento di dati personali” del GDPR

42 Pertanto sia nel caso in cui il soggetto agente sia consapevole della possibilità che l'evento possa verificarsi, e ne accetta il rischio (*dolo eventuale*), ovvero quando lo stesso agisce in malafede, ossia con espressa volontà e nella consapevolezza delle conseguenze delle proprie azioni o omissioni (*dolo o dolo premeditato*).

43 Il “reato presupposto” è una tipologia di delitto che, a sua volta, diventa propedeutico ad un altro atto colposo, ovvero da cui scaturisce e si configura un altro reato. Per approfondimenti in merito, si consiglia anche M. D'AGOSTINO PANEBIANCO, *L'evoluzione e le novità nel contrasto al riciclaggio: la VI Direttiva Europea*, in *Rivista Compliance*, ed. SEAC, n.5, 2021, pp.24-28

44 Ai fini di questo ragionamento, sarebbe assolutamente indifferente se si trattasse del reato di furto, nonostante le due fattispecie differiscano in ragione delle circostanze precedenti la commissione dello stesso: infatti, nel caso di furto, viene sottratto al terzo, un bene legittimamente posseduto; mentre nell'ipotesi di appropriazione indebita, l'autore del reato è già in possesso del bene di cui si appropria.

individuare la natura e caratteristiche dei “dati”, al fine di poter comprendere la fattispecie di reato.

Nell’ipotesi di appropriazione indebita di *files* contenenti “segreti” di natura aziendale od industriale, si incorrerebbe (quantomeno) nella violazione degli obblighi di riservatezza e fedeltà, rubricati all’articolo 2105 c.c., ovvero in taluni casi dell’articolo 622 c.p., se non anche integrando la condotta di concorrenza sleale⁴⁵.

Ed ancora, nell’ipotesi, che i dati siano “personali”⁴⁶, la sottrazione degli stessi in un contesto di trattamento per finalità lavorative, professionali o commerciali⁴⁷, presupporrebbe in via logica, anche l’assenza della base legale e/o del presupposto “consenso informato” per determinate finalità e modalità di trattamento⁴⁸: pertanto, in tale circostanza, il reato presupposto (furto o appropriazione indebita), integra l’illecito trattamento di dati personali.

Seguendo il medesimo filo logico, è da analizzare la classica configurazione del “*furto di identità*”: questa condotta consiste nella illecita acquisizione di una identità di una persona esistente⁴⁹, impossessandosi di quei dati ed informazioni (che, per qualità e quantità, sono sufficienti a rendere credibile agli occhi dei terzi l’“impersonificazione”) da database o sistemi di *storage* in cui sono conservati, ovvero carpirli utilizzando tecniche di intercettazione delle comunicazioni informatiche, come ad esempio, *webspoofting*, *man-in-the-middle*, *receptioning* delle email, etc.⁵⁰. Tale condotta si può concretizzare e descrivere attraverso due diverse modalità: l’“*impersonificazione totale*”⁵¹ o l’“*impersonificazione parziale*”⁵², oggigiorno facilmente attuabili, proprio in relazione ai moderni strumenti informatici, ed alle sempre più note tecniche di infrazione⁵³.

Dal punto di vista prettamente giuridico, se da un lato rientra certamente nella sottrazione di dati personali (e quindi vi è un illecito trattamento), dall’altro è una condotta riconducibile alla “sostituzione di persona”, rubricata all’Articolo 494 del codice penale⁵⁴, che sovente è

45 Si vedano anche le considerazioni finali, in calce al presente.

46 Così come dalla definizione data dall’Articolo 4, co. 1 del Regolamento UE n.2016/679.

47 Quali, a mero titolo esemplificativo e non esaustivo, sottraendo la lista dei clienti del precedente datore di lavoro, al fine di apportare un patrimonio informativo, finalizzato a mettere in atto una campagna mirata di contatto e marketing da parte della nuova impresa ove si lavora.

48 Che ciascun Titolare del trattamento deve ottenere, salvo i casi di legittimo interesse o assolvimento di un obbligo di legge.

49 Si noti che esiste una netta differenza con la creazione di una “falsa identità” (ossia non riferibile o riconducibile ad una persona esistente), come spesso accade, con una gravità spesso inferiore, creando *fake profiles*.

50 N. CHOU - R. LEDESMA - Y. TERAGUCHI - J. C. MITCHELL, *Client-Side Defense Against Web-Based Identity Theft*, NDSS Symposium, 2004

51 Ovvero, l’occultamento totale della propria identità mediante l’utilizzo indebito di dati relativi all’identità e al reddito di un altro soggetto, e può riguardare l’utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto.

52 Ovvero, l’occultamento parziale della propria identità mediante l’impiego, in forma combinata, di dati relativi alla propria persona e l’utilizzo indebito di dati relativi ad un altro soggetto.

53 L. TAMILSELVAN - V. SANKARANARAYANAN, *Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks*, in *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.3, 2007

54 “Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all’altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno”.

presupposto per la commissione o aggravante del reato di frode informatica⁵⁵, come peraltro più volte affermato dalla Corte di Cassazione, sezione penale⁵⁶. Inoltre, parlando di “*impersonation*”, non si può non richiamare una delle condotte tipiche del cyberbulling⁵⁷, quando l’*offender* – dopo essersi procurato le credenziali di accesso di un account della vittima, tipicamente di un social network – avvia una vera e propria campagna denigratoria⁵⁸ che crea imbarazzo alla vittima ovvero ne mina la reputazione.

5. Il rapporto tra IP, capitale umano ed i dati.

La “conoscenza” è sin dai tempi antichi uno degli stimoli e dei desideri più significativi nella vita dell’uomo: già nell’Antico Testamento, la Bibbia riporta⁵⁹ nella vicenda della tentazione del serpente, Adamo ed Eva si trovano davanti al rispetto di un comandamento (“non mangiate del frutto dell’albero che è in mezzo al giardino”), ma anche e soprattutto acquisire conoscenza poiché “l’albero era desiderabile per diventare intelligente”.

Fin dai tempi dei *dialoghi di Menone* di Platone, i filosofi si sono chiesti perché la conoscenza è più preziosa della mera credenza. Infatti, alcuni filosofi pensano anche che la conoscenza sia migliore della vera credenza e giustificano la vera credenza non solo in termini di grado, ma anche nella sua natura. Questa materia è di fondamentale importanza per le nostre vite come “esseri pratici e sociali”: infatti, la conoscenza è il mezzo principale per comunicare e ricevere le informazioni necessarie per pianificare, coordinare gli sforzi e, più in generale, vivere una vita prospera. Quindi, è importante per noi affermare le cose che dovremmo, e non affermare le cose che non dovremmo. Qualunque sia lo stato che ci permette di farlo è prezioso⁶⁰.

Lo sviluppo della società postindustriale e dell’informazione è caratterizzato dal modo in cui questi tipi di società pongono la “conoscenza” al centro delle loro relazioni economiche e sociali⁶¹, in cui il forte legame tra la conoscenza ed i dati, viene considerato come un elemento strategico da tutelare, nei più svariati ambiti pubblici e privati.

Per tale ragione, prima di entrare nel merito di alcuni approfondimenti, è opportuno soffermarsi su alcune definizioni, per condividere i significati ed avere quel quadro sufficiente per apprezzarne il valore. In precedenza sono già state fornite le definizioni di dato, informazioni e di capitale umano, in cui è stato evidenziato come questi sono assimilabili a beni immateriali, e dunque afferiscono anche al patrimonio aziendale, riferibile

55 Articolo 640 ter del Codice Penale.

56 In tal senso, si vedano a titolo esemplificativo, la Corte di Cassazione, Sezione Penale IV, sentenza 23 aprile 2014, n. 25774; Sezione Penale V, sentenza del 29 febbraio 2016, n. 8275.

57 Da notare che le fattispecie di reato che configurano il *cyber-bullismo* sono svariate, e possono essere poste in essere singolarmente o congiuntamente: queste sono, ad esempio, gli atti persecutori, ex art. 612-bis cp; la diffamazione aggravata, ex art. 595 cp; la molestia o disturbo della persona, ex art. 660 cp.; le minacce, ex art. 612 cp.

58 A mero titolo esemplificativo e non esaustivo, attraverso l’invio di messaggi o la pubblicazione di contenuti inopportuni.

59 Genesi, 3, 1-5

60 J. TURRI, *Knowledge And The Norm Of Assertion: An Essay in Philosophical Science*, New Publisher Ed., 2021, p.29

61 Si veda B. WESSELS - R.L. FINN - K. WADHWA - T. SVEINSDOTTIR - L. BIGAGLI - S. NATIVI - M. NOORMAN, *Open Data and the Knowledge Society*, Amsterdam University Press, 2017, p.175.

alla più ampia nozione di azienda (ossia, «*il complesso dei beni impiegati nel processo produttivo aziendale da parte dell'imprenditore*»⁶²), di cui all'Articolo 2555 Codice Civile.

La proprietà intellettuale (anche definita, come *Intellectual Property*, IP), secondo l'articolo 1.2 dell'«*Accordo relativo agli aspetti dei diritti di proprietà intellettuale attinenti al commercio*» (TRIPs)⁶³, ricomprende il Diritto d'autore e diritti connessi⁶⁴, i marchi⁶⁵, le indicazioni geografiche⁶⁶, i disegni industriali⁶⁷, i brevetti⁶⁸, le topografie di prodotti a semiconduttori⁶⁹, e le informazioni segrete⁷⁰. In questa sede è facilmente riscontrabile come vi sia una forte coincidenza con la definizione data dal Codice della Proprietà Industriale⁷¹ per la «proprietà industriale»⁷². È opportuno ricordare come «*i vari diritti di proprietà intellettuale hanno per oggetto beni naturalmente destinati ad un godimento plurimo e solidale e per i quali solo la legge può creare una situazione di scarsità attraverso l'attribuzione di diritti esclusivi*»⁷³.

In tal senso, il Codice della Proprietà Industriale prevede che la tutela dei diritti della proprietà industriale avvenga attraverso la brevettazione, mediante registrazione (o negli altri modi previsti dal Codice), dando luogo ai titoli di proprietà industriale.

Per una migliore comprensione del valore immateriale della conoscenza, nonché della sua strategicità, è opportuno rilevare come (in ambito aziendalistico), il tema dei beni immateriali venga, altresì, trattato dai principi contabili: nello IAS 38, che fornisce istruzioni su come determinarne il valore contabile, viene evidenziato come «*alcune attività immateriali possono essere contenute in oggetti di consistenza fisica quali per esempio un compact disc (nel caso di un software per computer), una documentazione legale (nel caso di una licenza o di un brevetto) o una pellicola*», escludendo il caso in cui il relativo software sia strumentale al funzionamento di un altro hardware⁷⁴. Rilevante, in tal senso, è la precisazione del punto 5, che dopo aver elencato puntualmente le attività rientranti⁷⁵ (spese di pubblicità, formazione, avvio, attività di ricerca e sviluppo), puntualizza che «*le attività di ricerca e sviluppo sono rivolte allo sviluppo di conoscenze. Conseguentemente, sebbene tali attività possano concretizzarsi in beni di consistenza fisica (per esempio, un prototipo), la componente fisica dell'attività risulta secondaria rispetto alla sua componente immateriale, ossia la conoscenza in esso contenuta*».

62 Brocardi.

63 Il «*Trade Related Aspects of Intellectual Property Rights*» è stato adottato a Marrakech 15 aprile 1994, e ratificato dall'Italia con legge 29 dicembre 1994, n. 747.

64 Cfr. sezione 1 del TRIPs.

65 Cfr. sezione 2 del TRIPs.

66 Cfr. sezione 3 del TRIPs.

67 Cfr. sezione 4 del TRIPs.

68 Cfr. sezione 5 del TRIPs.

69 Cfr. sezione 6 del TRIPs.

70 Cfr. sezione 7 del TRIPs.

71 Il Codice della Proprietà Industriale (a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273) è stato emanato con il Decreto Legislativo 10 febbraio 2005, n. 30.

72 Che all'articolo 1, ne definisce il perimetro ricomprendendo: i marchi ed altri segni distintivi, le indicazioni geografiche, le denominazioni di origine, i disegni ed i modelli, le invenzioni, i modelli di utilità, le topografie dei prodotti a semiconduttori, informazioni aziendali riservate e nuove varietà vegetali.

73 A.M. ROVATI, *op. cit.*, p.157.

74 In tal caso, tali attività dovranno essere trattate secondo le disposizioni dello IAS 16.

75 Alle quali devono essere aggiunte quelle rubricate al punto 6, quali «*Diritti detenuti dal locatario derivanti da accordi di licenze per oggetti quali filmati cinematografici, videocassette, opere teatrali, opere letterarie, brevetti e diritti d'autore*».

L'importanza e la strategicità della conoscenza, anche ai fini della competitività, è peraltro desumibile da alcune misure pubbliche di incentivo, quali a titolo esemplificativo il *Patent Box*, ossia «un regime opzionale di tassazione agevolata per i redditi derivanti dall'utilizzo di software protetto da copyright, di brevetti industriali, di marchi d'impresa (poi esclusi per le opzioni esercitate dopo il 31 dicembre 2016), di disegni e modelli, nonché di processi, formule e informazioni relativi a esperienze acquisite nel campo industriale, commerciale o scientifico giuridicamente tutelabili. [Questa misura, *nda*] consente a tutti i soggetti titolari di reddito d'impresa, indipendentemente dalla natura giuridica, dalla dimensione e dal settore produttivo di appartenenza, incluse le stabili organizzazioni in Italia di residenti in Paesi con i quali è in vigore un accordo per evitare la doppia imposizione e con i quali lo scambio di informazioni è effettivo, la parziale detassazione dei proventi derivanti dallo sfruttamento dei citati beni immateriali»⁷⁶.

In questo contesto, deve essere però evidenziato che l'evoluzione della società, in particolare quella che si esprime attraverso la dimensione digitale, ha portato anche alla creazione di modalità "ibride" (ossia, regolamentata in modo autonomo, spontaneo e parziale, in seguito ad un processo *bottom-up*), come ad esempio «le *Online Creation Communities (OCCs)*, sono aperte a qualsiasi utente anonimo che desidera contribuire, mentre altre hanno avvertimenti sull'identificazione dei partecipanti o escludono utenti antisociali o dirompenti, come i troll. [...] Le limitazioni al flusso di informazioni personali o all'utilizzo da parte di estranei proteggono anche il valore delle risorse di conoscenza per i beneficiari previsti, siano essi membri della comunità o il pubblico in generale. Molti di questi "knowledge common" vietano l'uso commerciale delle informazioni personali condivise all'interno della comunità perché tali usi secondari al di fuori della conoscenza o del consenso degli interessati originali potrebbero presentare alcuni rischi per i partecipanti»⁷⁷.

Si può ben comprendere, dunque, come il dato (o l'informazione) non possa essere considerato esclusivamente come una "componente informatica o digitale", bensì piuttosto come il supporto che contiene la rappresentazione della conoscenza ed il know-how, e per conseguenza le misure di sicurezza atte a garantirne la disponibilità, integrità e riservatezza, non afferiscono esclusivamente alla sfera della *cybersecurity*, bensì sono strumentali alla tutela e corretto sfruttamento, anche ai fini economici e commerciali, dei relativi diritti.

6. Una considerazione conclusiva su due rischi derivanti.

Dal quadro *supra* delineato emerge chiaramente come l'instaurazione di un qualsivoglia rapporto di lavoro - sia esso subordinato, o di altra natura - si fonda sulla reciproca lealtà ed affidabilità.

Questo è maggiormente vero in tutte quelle circostanze in cui il contesto in cui si sviluppa la relazione è incentrato sulle "*corporate information and data*" e sullo sviluppo di *know-how*, e *knowledge* finalizzato allo sfruttamento imprenditoriale. Pertanto, in un contesto di "patrimonializzazione del dato", emergono evidenti due rischi che sebbene distinti,

⁷⁶ come riportato da una descrizione dell'Agenzia delle Entrate.

⁷⁷ M. SANFILIPPO - B. FRISCHMANN - K. STANDBURG, *Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework*, in *Journal of Information Policy*, 2018, Vol. 8, p.138.

rappresentano le due facce della medesima medaglia⁷⁸. Una esemplificazione può aiutare ad illustrare e meglio comprendere la questione.

Nel corso di un rapporto di lavoro (*in itinere*), l'impresa affida al proprio lavoratore non solo dei task da eseguire, ma rivela (a) modalità ed (b) informazioni utili ed indispensabili per il raggiungimento di obiettivi: la combinazione tra i due elementi non solo arricchisce il "capitale umano", ma diventa un pericoloso rischio a violare quel patto di lealtà⁷⁹ che è alla base della relazione stessa.

D'altro canto, il citato rischio non cessa nel momento in cui si interrompe la relazione: infatti, una simile violazione della lealtà potrebbe materializzarsi tanto come logica prosecuzione della condotta illecita testé descritta, ma anche come una nuova ed autonoma, che potrebbe configurare la condotta di "concorrenza sleale". Invero, l'infedele essendo a conoscenza di informazioni e dati potrebbe agire in danno della precedente controparte, con un livello di efficacia molto elevato.

Pertanto, in una logica di *risk management* l'impresa deve attuare (*ex ante*) una politica preventiva per mitigare il "rischio di infedeltà", attuando sin dalla instaurazione del rapporto adeguati presidi⁸⁰ (tanto contrattuali⁸¹, quanto organizzativi⁸² e ICT⁸³) atti ridurre la possibilità di successo di una potenziale azione fraudolenta.

Bibliografia

- ARZIA G., *Statistica, nuovo empirismo e società nell'era dei Big Data*, Nuova Cultura Ed., 2018.
- CHOU N. - LEDESMA R.- TERAGUCHI Y. – MITCHELL J. C., *Client-Side Defense Against Web-Based Identity Theft*, NDSS Symposium, 2004
- D'AGOSTINO PANEBIANCO M., *From "corporate disloyalty" to "unfair competition"*, in *Rivista Giuridica AmbienteDiritto.it*, 2019, n.4
- D'AGOSTINO PANEBIANCO M., *Vivere nella Dimensione Digitale*, Themis ed., 2019
- D'AGOSTINO PANEBIANCO M., *L'evoluzione e le novità nel contrasto al riciclaggio: la VI Direttiva Europea*, in *Rivista Compliance*, ed. SEAC, n.5, 2021
- DI TULLIO D'ELISIA A., *I dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale*, in *Diritto&Diritti*, 2020
- FLORIDI L., *Pensare l'infosfera, la filosofia come design concettuale*, Raffaello Cortina Ed., 2020.
- JONA-LASINIO C., *Il capitale immateriale e i territori italiani*, in AA.VV., *5° Rapporto sulla classe dirigente*, Rubettino Editore, 2011
- PAGELLA C., *La Cassazione sulla riconducibilità dei file al concetto di "cosa mobile" oggetto di appropriazione indebita: un caso di analogia in malam partem?*, in *Sistema Penale*, 2021.

78 Per un approfondimento in merito, si rinvia a M. D'AGOSTINO PANEBIANCO, *From "corporate disloyalty" to "unfair competition"*, in *Rivista Giuridica AmbienteDiritto.it*, 2019, n.4, pp. 42-53.

79 In tal senso è opportuno richiamare il Codice Civile all'art. 2105 (Obbligo di fedeltà) secondo cui, *expressis verbis*, «il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio».

80 In tal senso è opportuno richiamare Brocardi «il dovere di fedeltà impone l'osservanza di due obblighi di natura negativa: a) divieto di concorrenza; b) obbligo di riservatezza» per individuare le componenti essenziali su implementare tali presidi.

81 *Inter alia*, individuando apposite clausole contrattuali.

82 *Inter alia*, attenuando i potenziali conflitti d'interesse nonché implementando procedure di *segregation of duties*.

83 *Inter alia*, prevedendo misure tecniche che limitino (ove non strettamente necessario) l'effettuazione di copie e/o la trasmissione di informazioni e dati.

- PAPA BENEDETTO XVI, *Lettera Enciclica Caritas In Veritate*, Vaticano, 29 giugno 2009
- PISANI N., *La nozione di "cosa mobile" agli effetti penali e i 'files' informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in *Diritto penale e processo*, 5/2020
- ROVATI A.M., *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici*, in *Rivista Informatica e diritto*, Vol. XX, 2011, n. 1-2
- SANFILIPPO M. - FRISCHMANN B. - STANDBURG K., *Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework*, in *Journal of Information Policy*, 2018, Vol. 8
- SPINOSA A., *Il cigno nero". Diritti, potere e libertà di fronte al silenzio della legge. Un dibattito teorico di primo novecento*, in *Historia et Ius*, 2020, n.18
- TALEB N. N., *The Black Swan: The Impact of the Highly Improbable*, Penguin Books, 2008
- TAMILSELVAN L.- SANKARANARAYANAN V., *Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks*, in *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.3, 2007
- TURRI J., *Knowledge And The Norm Of Assertion: An Essay in Philosophical Science*, New Publisher Ed., 2021
- VISCO I., *Capitale umano e crescita (Intervento del Governatore della Banca d'Italia)*, Università Cattolica del Sacro Cuore, 30 gennaio 2015
- WESSELS B.- FINN R.L. - WADHWA K. - SVEINSDOTTIR T. - BIGAGLI L. - NATIVI S. - NOORMAN M., *Open Data and the Knowledge Society*, Amsterdam University Press, 2017
- ZICCARDI G., *Legal Tech Books (S01 E03) Francesca Rossi, "Il confine del futuro"*, 2020.