RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0174 • articolo sottoposto a peer review • pubblicato in anteprima il 25 nov. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Riccardo Michele Colangelo

Ne pereant fragmenta: l'intelligenza artificiale e la complessità della *Corptech governance*

Il crescente utilizzo delle tecnologie digitali nell'esercizio di attività d'impresa comporta significative questioni di cyberdiritto societario. Anche nello specifico ambito dei c.d. rischi tecnologici d'impresa, l'apporto dell'informatica giuridica e l'approccio metodologico del giurista informatico possono agevolare un'indagine più completa degli elementi di complessità che caratterizzano le nuove tecnologie, agevolando al contempo l'adeguatezza degli assetti societari. A margine della definitiva approvazione dell'AI Act, il presente contributo intende approfondire tali considerazioni in tema di *Corptech governance*, con particolare riguardo all'uso di sistemi di intelligenza artificiale, evidenziando anche profili di *data protection* e sicurezza informatica, nonché le ricadute sugli assetti. Lungi dalle logiche di una mera opera ricognitiva, si intende sottolineare l'esigenza di superare l'approccio formalistico talora emergente in sede di *compliance* normativa, valorizzando il ruolo degli assetti digitali ed aprendo la via ad una non procrastinabile attenzione ai profili di *Corporate Digital Responsibility*.

Intelligenza artificiale – Corptech governance – Informatica giuridica – Assetti societari
Corporate Digital Responsibility

Ne pereant fragmenta: artificial intelligence and the complexity of Corptech governance

The rise in the use of digital technologies in business activities brings up significant issues about corporate cyberlaw. Also in the specific field of the so-called technological risks of business, legal informatics and IT jurist's methodological approach can enable a broader examination of the complexity associated with new technologies, while facilitating the adequacy of corporate structures. After a brief period following the final approval of the AI Act, this paper intends to deepen these relevant issues regarding Corptech governance, focusing on the use of artificial intelligence systems and highlighting data protection and cybersecurity concerns, along with the impact on corporate structures. This paper also aims to emphasise the need to overcome the formalistic approach sometimes arising in the context of regulatory compliance, paving the way for an unpostponable focus on Corporate Digital Responsibility.

Artificial intelligence – Corptech governance – Legal informatics – Corporate structures
Corporate Digital Responsibility

L'Autore è dottorando di ricerca presso Universitas Mercatorum, Roma

Sommario: 1. Attività d'impresa e tecnologie digitali. – 2. Il giurista informatico e l'intelligenza artificiale. – 3. Brevi note sui profili giuridici di complessità dell'IA. – *3.1. Dalla* data protection... – *3.2. ...alla sicurezza informatica*. – 4. Alcuni spunti circa l'adeguatezza degli assetti digitali. – 5. Il ruolo della *Corporate Digital Responsibility*.

1. Attività d'impresa e tecnologie digitali

Il crescente ricorso, nell'ambito dell'esercizio collettivo di attività d'impresa, all'utilizzo delle tecnologie digitali, ancora oggi caratterizzato da ampi margini di perfettibilità e fortemente auspicato e stimolato anche a livello eurounitario, non può essere apprezzato appieno, nei suoi risvolti giuridici, limitandosi ad analisi quantitative e ad osservazioni meramente fattuali[1].

Queste ultime, d'altra parte, sebbene talora condizionate da alcuni vincoli metodologici non del tutto condivisibili, consentono quantomeno di stimare, grazie a dati statisticamente rilevanti, la concreta diffusione di determinate tecnologie nello specifico contesto societario[2].

Pur prescindendo dai profili eminentemente quantitativi, l'impiego di tecnologie digitali – che talora viene percepito quale vero e proprio limite all'avvio di una nuova attività imprenditoriale[3] – risulta di norma caratterizzato da non pochi corollari giuridicamente rilevanti, continuando a porre, per quanto interessa maggiormente in questa sede, stimolanti questioni di cyberdiritto societario.

1. Sia sufficiente, in proposito, il rimando all'ultimo (e primo) *Report on the state of the Digital Decade 2023*, pubblicato dalla Commissione europea nel mese di settembre 2023 (cfr. European Commission 2023-a) e che *de facto* subentra al *Digital Economy and Society Index* (DESI), ove non emergono dati particolarmente lusinghieri circa l'attuale ricorso alle tecnologie in ambito societario, in modo speciale per quanto concerne le PMI. Il Rapporto è stato introdotto dalla Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030. Per quanto maggiormente interessa in questa sede, la decisione *de qua*, all'art. 4, par. 1, n. 3, prevede specifici obiettivi in materia di «trasformazione digitale delle imprese»: il ricorso, da parte di «almeno il 75 % delle imprese dell'Unione, in base alle proprie esigenze aziendali», alternatamente a servizi di cloud computing, big data e/o intelligenza artificiale; il raggiungimento quantomeno di un «livello base di intensità digitale» da parte di «oltre il 90% delle PMI dell'Unione»; l'agevolazione da parte dell'Ue di "scale-up innovative" favorendo «il loro accesso ai finanziamenti, almeno raddoppiando il numero di aziende unicorni». In dottrina, per tutti, si vedano Matricano 2020 e Pascucci 2017, p. 5 ss.
2. Nel *Report on the state of the Digital Decade 2023. Annex Italy*, con particolare riguardo ai dati concernenti il contesto italiano, risulta preso in considerazione l'utilizzo di tecnologie digitali "avanzate" e, in relazione ai soli sistemi di intelligenza artificiale, si quantifica nella misura del 6% la quota di società che vi hanno fatto ricorso nel 2021: cfr. European Commission 2023-b. Più articolata, invece, la *Rilevazione sulle tecnologie dell'informazione e della comunicazione (Ict)* dell'ISTAT, pubblicata il 4 gennaio 2023 e riferita all'anno precedente, che tuttavia non contempla indicatori non secondari, quali «intelligenza artificiale e big data», in quanto, «ad oggi, demandati ad altre fonti di statistica non ufficiale» (così ISTAT 2023, p. 18).
3. Cfr. Unioncamere – ANPAL 2023, pp. 26, 65 e 102. Più in generale, in merito alla propensione imprenditoriale ed all'avvio di nuove imprese, si rinvia ai dati riportati in Micozzi 2024.

Queste ultime, da un lato, hanno la potenzialità di interrogare, in ultima analisi, anche taluni principi fondamentali della disciplina di settore; dall'altro, non necessariamente coinvolgono *in toto*, e quindi in modo esclusivo e diretto, specifici istituti del diritto commerciale. In argomento, limitando l'analisi ai profili giuridicamente rilevanti, meritano un'adeguata (ri)valutazione anche quelli che indirettamente – ma non in via secondaria – riguardano l'ambito societario, caratterizzati peraltro da risvolti evidenziabili anche in un'ottica di *risk management*[4], così come informatico-giuridica.

2. Il giurista informatico e l'intelligenza artificiale

In argomento, se è vero che una qualificata attenzione dottrinale allo studio dei fenomeni tecnologici non costituisce più appannaggio del tradizionale settore informatico-giuridico, l'approccio metodologico proprio del giurista informatico, attento a cogliere e valorizzare la rilevanza anche di profili interdisciplinari[5], consente a tutt'oggi, anche in ambiti specifici come quello del diritto societario, non solo di ampliare il campo dell'analisi, ma anche – e soprattutto – di indagare più compiutamente quegli elementi di complessità che, agli occhi del giurista, caratterizzano le nuove tecnologie[6].

Tali considerazioni, riferibili al ricorso tanto all'intelligenza artificiale – tema particolarmente attuale, significativamente attenzionato dalla più recente dottrina[7] – quanto ad altre tecnologie digitali, siano esse strumento o oggetto di governo dell'impresa[8], risultano preziose nell'ambito della *Corptech governance*[9], consentendo non solo di apprezzare meglio talune singole tessere, ma anche di scorgere intere porzioni dell'ideale mosaico del cyberdiritto societario. Il tutto con ricadute effettive a beneficio dell'organo gestorio, ai fini di una corretta – e non parziale – strutturazione degli assetti societari, con particolare riguardo a quelli digitali[10], senza sottostimare quanto pertiene non solo alla valutazione dei rischi, ma anche – e soprattutto – alla gestione dei medesimi.

3. Brevi note sui profili giuridici di complessità dell'IA

Più nello specifico, i preconizzati profili di complessità possono scaturire tanto dalla concreta applicabilità, sia essa alternativa o concorrente, di plurime discipline specifiche[11], quanto da vuoti normativi relativi all'utilizzo di strumenti informatici di uso ormai corrente. In argomento, oltre alla contingente assenza di disciplina positiva, peraltro non aliena al rapporto tra diritto e nuove tecnologie, caratterizzato di norma da un fisiologico ritardo

4. Tra la più autorevole dottrina giuridica in tema di *risk management* e tecnologie digitali si veda, per tutti, Cerrato 2019.
5. Cfr. Borruso-Russo-Tiberi 2009, p. 2.
6. In argomento, si consenta di evocare la rilevanza dell'"approccio informatico-giuridico *by design*", proposto in Colangelo 2023, p. 115.
7. *Ex multis*, e senza pretese di completezza, cfr. Bianchini–Gasparri–Resta et al. 2022; Schneider 2022, p. 711 ss.; Abriani–Schneider 2021; Mosco 2019, p. 247 ss.; Enriques–Zetzsche 2019.
8. Cfr. Abriani–Schneider 2021, p. 191 ss. e 235 ss.
9. Cfr. Liberanome 2022, p. 94 e Scarchillo 2019, p. 881 ss.
10. In argomento, si veda il riferimento agli "assetti cibernetici" riportato in Cerrato–Culasso–Crocco 2023, pp. 318-319.
11. Si pensi, in argomento, all'emblematico caso dei criptoasset ed alla limitata portata del regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività (meglio noto con l'acronimo inglese MiCAr), che, all'art. 2, par. 4, riconosce *expressis verbis* l'esclusione dall'ambito di applicazione del regolamento medesimo di un novero piuttosto ampio "cripto", se ed in quanto queste ultime integrano fattispecie già oggetto di una specifica disciplina. A titolo esemplificativo, è questo il caso – certamente non "di scuola" – delle cripto-attività che rientrano nella definizione di strumenti (*rectius*: prodotti) finanziari, in relazione alle quali il successivo comma 5 prevede, entro il 30 dicembre 2024, l'elaborazione, da parte dell'ESMA, di «orientamenti conformemente all'articolo 16 del Regolamento (UE) n. 1095/2010 sulle condizioni e sui criteri per la qualificazione delle cripto-attività come strumenti finanziari».

del legislatore[12] – ben possono assumere rilevanza anche i casi in cui l'iter normativo, seppur avviato, non si sia ancora concluso, così come quelli, non infrequenti soprattutto nel contesto delle fonti di secondo livello del diritto unionale, caratterizzati da una significativa *vacatio*, talora biennale, tra l'entrata in vigore e la concreta applicabilità di una determinata disciplina[13].

Ciò risulta particolarmente evidente anche operando una sorta di *actio finium regundorum* relativamente all'oggetto delle presenti note, prendendo in considerazione il peculiare e fertile campo dei sistemi di intelligenza artificiale.

Tale ambito, infatti, è risultato a lungo caratterizzato dall'assenza di una disciplina specifica, nelle more della definitiva approvazione del regolamento europeo in materia, noto come AI Act[14].

D'altra parte, l'entrata in vigore di quest'ultimo, intervenuta poco prima della definitiva chiusura delle presenti note, ha per ora consacrato una disciplina che solo gradualmente potrà essere considerata vincolante e, in quanto tale, incidere sullo sviluppo e sull'utilizzo di sistemi di intelligenza artificiale: infatti, il regolamento (UE) 2024/1689 del 13 giugno 2024, pubblicato il successivo 12 luglio[15] ed entrato in vigore venti giorni dopo, sarà pienamente applicabile, nella sua interezza, solo il 2 agosto 2027[16].

Cionondimeno, l'attuale assenza di uno specifico *corpus* di norme giuridiche vincolanti in materia di intelligenza artificiale non può giustificare – in special modo nel contesto dell'adozione di siffatta tecnologia in ambito societario – un entusiastico ma semplicistico "*Omnia licent!*"[17], foriero di una potenziale significativa esposizione a rischi e a responsabilità.

Seppur in assenza di cogenti obblighi normativi, lo stato sempre più avanzato dell'iter legislativo dell'AI Act, culminato con la recentissima approvazione e la successiva entrata in vigore, evidenzia con singolare chiarezza la crescente opportunità di non sottovalutare, in un'ottica proattiva, quantomeno le direttrici della normativa specifica.

Queste ultime, ad onor del vero, avrebbero già potuto essere prese in considerazione – in attesa della pubblicazione del testo definitivo – per come desumibili in concreto dalla disamina dei rilevanti emendamenti alla proposta di AI Act approvati dal Parlamento europeo nel mese di giugno 2023[18], così come dell'ancor più attendibile testo

12. *Ex multis*, cfr. Pietrangelo 2007, p. 176, ove peraltro si evidenziano anche i principali profili problematici di tale tendenziale ritardo, e Rolli 2018, pp. XVIII-XIX.
13. Cfr. art. 297 TFUE. Una *vacatio* biennale caratterizza in concreto l'applicabilità del Regolamento generale sulla protezione dei dati personali (2016/679 del 27 aprile 2016), noto con l'acronimo inglese GDPR: entrato in vigore nel 2016, il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea, è divenuto pienamente applicabile solo il 25 maggio 2018, come espressamente previsto *ex* art. 99, parr. 1 e 2.
14. Commissione europea, Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, COM(2021) 206.
15. Si tratta del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale).
16. Ai sensi dell'art. 113, pur essendo disposta *expressis verbis* la piena applicabilità del regolamento a decorrere dal 2 agosto 2026, sono previste alcune eccezioni, che anticipano – e, in un caso, posticipano – l'applicabilità di alcune norme dell'AI Act. Tali deroghe risultano così formulate alle lettere a)-c): «a) I capi I e II si applicano a decorrere dal 2 febbraio 2025; b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101; c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal 2 agosto 2027».
17. «*"Omnia licent!". Sed non omnia expediunt. "Omnia licent!". Sed non omnia aedificant*» (1 Cor 10,23). In dottrina, in senso sostanzialmente conforme, cfr. Borruso–Russo–Tiberi 2009, p. 582, ove si evidenziano gli "ingenui entusiasmi" talora connaturati all'adozione delle tecnologie informatiche.
18. Parlamento europeo, emendamenti, approvati il 14 giugno 2023, alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM(2021)206 – C9-0146/2021 – 2021/0106(COD)).

consolidato in esito alla risoluzione legislativa del Parlamento europeo del 13 marzo 2024[19].

A ciò si aggiunga un ulteriore – e fondamentale – rilievo: fatta salva la doverosa ed indiscussa applicazione delle norme dell'AI Act a far data da quando, progressivamente, diverranno del tutto vincolanti, le finestre di non applicabilità della nuova disciplina – in maniera non dissimile dalla precedente assenza del quadro normativo specifico in materia di intelligenza artificiale – non possono costituire un'esimente per quanto attiene all'applicazione di quelle ulteriori e differenti norme già in vigore, siano esse di matrice eurounitaria o meno, che, pur non dettate con diretto ed esclusivo riguardo ai sistemi di intelligenza artificiale, possono – *rectius*: debbono – comunque trovare applicazione anche in relazione al corretto utilizzo di questi ultimi, nelle grandi imprese così come nelle PMI.

3.1. Dalla *data protection*…

È questo il caso della normativa vigente in materia di *data protection*: con particolare riguardo al GDPR, è possibile affermare, in prima approssimazione, come il medesimo risulti *ex se* applicabile ai trattamenti di dati personali posti in essere nell'ambito dell'esercizio collettivo di attività d'impresa[20].

Più specificamente, non è dato dubitare circa l'applicabilità del Regolamento generale sulla protezione dei dati anche a quei trattamenti caratterizzati dal ricorso a sistemi di intelligenza artificiale[21], sebbene questi ultimi, all'interno del GDPR, non siano oggetto di alcun espresso ed univoco riferimento testuale.

Di converso, e sempre argomentando *de iure condito*, l'AI Act racchiude in sé, complessivamente, 30 espressi rinvii al GDPR, di cui 14 nei considerando e nelle relative note, altrettanti nell'articolato e 2 negli allegati, peraltro senza significative variazioni rispetto al precedente testo provvisorio, consolidato in esito agli emendamenti approvati dal Parlamento europeo.

Sul punto, in un'ottica diacronica, è dato osservare una crescita di siffatti riferimenti, laddove il dato quantitativo appena illustrato risulta maggiore rispetto non solo agli sparuti riferimenti al GDPR presenti nel testo originario della proposta di AI Act, ma anche alle 21 ricorrenze rinvenibili negli emendamenti approvati nel mese di giugno 2023.

Tra i riferimenti espressi al regolamento (UE) 2016/679, molti risultano operati all'interno di considerando e riferiti, in gran parte, ai dati biometrici.

Guardando all'articolato vero e proprio, emergono anche riferimenti a specifici istituti, già in precedenza definiti *ex* art. 4 GDPR. Tra di essi, nel vigente AI Act – così come nel testo della proposta di regolamento, come emendata nel 2024 – spiccano quelli riferiti ai dati biometrici (richiamati dall'art. 3, par. 1, punto 34), alle categorie particolari di dati personali (punto 37) ed alla profilazione (punto 52). Risultano, inoltre, riscontrabili anche le definizioni *per relationem* di dati personali e non personali, rispettivamente riportate ai punti 50 e 51 del medesimo art. 3, par. 1.

Più in generale, l'analisi del dato testuale consente di affermare come il GDPR non risulti richiamato dall'AI Act solamente per ragioni di tecnica normativa, correlate all'esigenza di attingere a definizioni già coniate nell'ambito della disciplina della *data protection* e fatte proprie dal nuovo regolamento.

In argomento, va dato atto non solo della conferma dell'impregiudicata applicabilità del Regolamento generale sulla protezione dei dati, prevista *expressis verbis* dal vigente art. 2, par. 7[22], ma anche di ben più rilevanti richiami ad istituti specifici.

19. Parlamento europeo, risoluzione legislativa del 13 marzo 2024 sulla proposta di AI Act.
20. In argomento, tra i vari contributi editi, sovente di carattere introduttivo, si vedano Miotto 2023 e Ciccia Romito 2021.
21. Si pensi al caso della videosorveglianza intelligente, peraltro contraddistinto da ulteriori elementi di complessità, dovuti alla potenziale rilevanza anche giuslavoristica del tema: cfr. Soffientini 2023, p. 245 ss.
22. Tale esplicitazione risulta essere stata inserita dagli emendamenti approvati dal Parlamento europeo nel mese di giugno 2023, mediante l'art. 2, par. 5 *bis*, della proposta di regolamento sull'AI, che disponeva quanto segue: «Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai trattamenti di dati personali in relazione ai diritti e agli obblighi stabiliti nel presente regolamento. Il presente regolamento lascia impregiudicati i regolamenti (UE) 2016/679 e (UE) 2018/1725

È questo il caso di quanto attiene alla valutazione d'impatto sulla protezione dei dati (o DPIA – *Data Protection Impact Assessment*[23]); in materia, oltre al richiamo di cui all'art. 26, par. 9, rivolto ai *deployer* di sistemi di intelligenza artificiale ad alto rischio, rileva anche il successivo art. 27, interamente dedicato alla disciplina di un'altra valutazione d'impatto, quella «sui diritti fondamentali per i sistemi di IA ad alto rischio».

In esso emergono alcuni significativi punti di contatto tra le due discipline, che meritano di essere evidenziati e valorizzati: al par. 4, in particolare, si dispone che, «se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 integra tale valutazione d'impatto sulla protezione dei dati».

Si tratta, in concreto, di una previsione normativa che mira ad una ottimizzazione degli adempimenti, evidenziando, al contempo, non solo l'imprescindibile coerenza contenutistica tra le due differenti valutazioni, ma anche – e soprattutto – l'opportunità di una valutazione caratterizzata da una più ampia visuale, che sappia cogliere, anche dalla normativa in materia di *data protection*, elementi di potenziale interesse per un'ottimale valutazione – e gestione – dei rischi sui diritti fondamentali.

In merito al rispetto del principio generale di trasparenza previsto dal GDPR, il vigente art. 50, par. 3, contempla per i *deployer* – abbandonando il termine "utenti"[24] – «di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica», l'obbligo di informazione delle persone fisiche coinvolte «in merito al funzionamento del sistema», anche se non più «in modo tempestivo, chiaro e comprensibile» e senza che venga espressamente richiamato il riferimento al consenso, precedentemente riscontrabile[25].

A latere, è sempre l'art. 50, par. 3, a confermare – in modo ridondante – l'obbligo, per tali *deployer*, di conformarsi, nel trattare i dati personali mediante siffatti specifici sistemi di intelligenza artificiale, alla normativa eurounitaria in materia di *data protection*.

Più ampiamente, in argomento, risulta meritevole di attenzione l'art. 86 dell'AI Act, rubricato *Diritto alla spiegazione dei singoli processi decisionali*, non presente nella originaria proposta di regolamento ed il cui disposto riproduce, con modificazioni, quello dell'art. 68 *quater*, introdotto nel mese di giugno 2023 ad opera dell'emendamento n. 630. Al par. 1, infatti, si sancisce il diritto di «qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio […] e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali

e le direttive 2002/58/CE e (UE) 2016/680, fatte salve le disposizioni di cui all'articolo 10, paragrafo 5, e all'articolo 54 del presente regolamento». Si noti come, nell'ultimo testo emendato prima della definitiva approvazione del regolamento, il disposto del paragrafo in questione, rinumerato, risultasse sostanzialmente invariato, eccezion fatta per il rinvio all'art. 59, in luogo dell'art. 54, poi confluito definitivamente nell'art. 2, par. 7, attualmente in vigore.

23. Tale istituto viene richiamato anche dal vigente art. 59, par. 1, lett. c), analogamente a quanto rinvenibile nell'ultimo testo disponibile della proposta di regolamento, mentre, in precedenza, era contemplato dall'art. 54, par. 1, lett. c) della proposta, come modificata dall'emendamento n. 510 approvato a giugno 2023. La norma, ora, riporta riferimenti a «meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento».
24. Come, invece, emergeva nel disposto dell'art. 52, par. 2, anche in esito alla modifica ad opera dell'emendamento n. 485, approvato nel mese di giugno 2023.
25. Non risultano ricomprese nel vigente disposto dell'articolo *de quo* anche queste specificazioni, introdotte sempre ad opera dell'emendamento n. 485, concernenti le modalità di veicolazione delle informazioni e la predeterminazione del consenso dell'interessato quale base giuridica dello specifico trattamento.

[…] di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata».

Interessante anche il caso dell'art. 10, par. 5[26], ove oggi si stabiliscono le condizioni da osservare obbligatoriamente e congiuntamente al fine di rendere possibile e lecito, seppur in via eccezionale, il trattamento di categorie particolari di dati personali, «nella misura in cui ciò sia strettamente necessario al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio».

Infine, nel 2023, durante l'iter di approvazione della proposta di regolamento, era stata introdotta nel nuovo punto 4 *bis* dell'allegato IV, ove si enumerano i contenuti della documentazione tecnica prevista nei casi di cui all'art. 11, par. 1, l'obbligatorietà di una «dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680», nei casi in cui un sistema di AI comporta il trattamento di dati personali[27]; tale dichiarazione risulta, oggi, ancora espressamente prevista dal vigente AI Act, sebbene attualmente riportata al punto 5 dell'Allegato V, relativo alla dichiarazione di conformità UE.

Ciò posto, pur prescindendo da più o meno significativi richiami testuali, talora riferiti solamente a talune categorie di sistemi di IA, è ben possibile affermare che, ad oggi, non vi possono essere dubbi in relazione all'applicabilità della vigente disciplina eurounitaria in materia di *data protection* a quei trattamenti che, nell'esercizio di attività d'impresa, già contemplano, anche solo in parte, il ricorso a siffatta tecnologia.

In altre parole, un utilizzo strumentale dell'intelligenza artificiale nel contesto di specifici trattamenti di dati non pare in alcun modo poter escludere l'applicabilità del GDPR, sussistendo gli elementi che determinano l'ambito di applicazione materiale o territoriale di quest'ultimo[28] e, comunque, purché si tratti di dati personali, per tali intendendosi, a mente dell'art. 4, par. 1, n. 1), GDPR, informazioni di qualsivoglia natura riguardanti «una persona fisica identificata o identificabile» e, quindi, un "interessato".

Proprio su questo punto, peraltro, si gioca una delle sfide più rilevanti, seppur non tra le più note e adeguatamente attenzionate – tanto nella prassi imprenditoriale, quanto a livello dottrinale – concernente l'anonimizzazione dei dati personali (o, *ab initio*, la natura non personale dei dati medesimi), che reca con sé, quale rilevantissimo corollario, l'inapplicabilità della disciplina in materia di *data protection*[29].

Posto che, *ex lege*, la natura personale del dato può derivare anche da una mera potenziale ed indiretta identificabilità dell'interessato, l'anonimizzazione, a maggior ragione con particolare riguardo a database particolarmente ricchi ed articolati, non può essere perseguita mediante modalità semplicistiche, quali la mera omissione di nomi e cognomi.

In argomento, il Regolamento generale sulla protezione dei dati personali non pare fornire significativi elementi all'interprete, né contribuire a delineare standard condivisi finalizzati a valutare e gestire il rischio di reidentificazione degli interessati, limitandosi ad operare, al considerando 26, un puntiforme riferimento alla nozione di sufficientemente anonimizzazione di dati personali[30].

26. Il paragrafo è stato modificato nel 2023 dall'emendamento n. 290 e, più di recente, nella sopra richiamata risoluzione legislativa del Parlamento europeo del 13 marzo 2024, ad opera della quale sono stati introdotti non solo riferimenti al GDPR, ma anche le condizioni che devono sussistere congiuntamente ai fini della liceità dello specifico trattamento, come definitivamente consacrate nel testo vigente.
27. Così l'emendamento n. 762 alla proposta di regolamento.
28. Cfr. artt. 2 e 3 GDPR.
29. Giova precisare che la non applicabilità del Regolamento generale sulla protezione dei dati non implica una assenza di disciplina specifica, la quale va individuata nel regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
30. Tale nozione può essere maggiormente delineata evidenziando i confini con quella di pseudonimizzazione, alla luce anche della più recente elaborazione giurisprudenziale in materia e, in particolare, della sentenza pronunciata dal Tribunale eurounitario il 26 aprile 2023, nella causa T-557/20.

Ulteriori e più specifici spunti possono essere tratti dal parere del Gruppo di lavoro articolo 29 n. 5/2014 sulle tecniche di anonimizzazione (WP216)[31], in particolare per quanto concerne gli aspetti metodologici ed applicativi della randomizzazione e della generalizzazione, intese quali macrocategorie, all'interno delle quali sono individuate plurime tecniche.

Più in generale, l'approccio del WP216 risulta basato su una valutazione ulteriore rispetto a quelle sinora richiamate, avente direttamente ad oggetto il rischio di reidentificazione, in modo non dissimile da quanto emerge dalla recentissima ISO/IEC 27559:2022 (*Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework*), norma tecnica di fondamentale importanza anche per quanto concerne il ricorso ad una nozione piuttosto relativa, quasi personalizzata, di anonimizzazione.

Nel contesto sinora illustrato, perseguire una sufficiente anonimizzazione dei dati personali e mantenere la medesima nel comunicare a terzi o nel diffondere i dataset in questione può risultare una singolare sfida, anche di natura tecnica, in particolare laddove la circolazione stessa dei dati non personali avvenga per finalità eminentemente commerciali, così come – per quanto interessa maggiormente in questa sede – nei casi in cui venga effettuata ai fini dell'apprendimento o dell'applicazione di sistemi di intelligenza artificiale.

Inoltre, tra le tante questioni giuridicamente rilevanti che pone e porrà il ricorso all'intelligenza artificiale, vi è pure quella della trasparenza (o della conoscibilità, secondo la terminologia preferita nella giurisprudenza amministrativa[32]), anche in relazione ai profili rilevanti in materia di *data protection*.

Sul punto, prescindendo dai riferimenti espressi attualmente presenti nel testo vigente dell'AI Act, può risultare utile richiamare un recente chiarimento dell'Autorità Garante per la protezione dei dati personali[33].

Si tratta di un "decalogo" che contempla alcune indicazioni per la corretta ed effettiva applicazione della normativa in materia di protezione dei dati personali, in relazione a quanto pertiene alla «realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale».

La disamina di tale testo consente di trarre alcuni significativi primi spunti, che peraltro paiono in grado di travalicare quanto direttamente concerne l'ambito sanitario: in altri termini, tale elaborazione dell'Autorità Garante per la protezione dei dati personali non solo può agevolare la comprensione delle peculiarità dei trattamenti di dati personali operati tramite strumenti di intelligenza artificiale, ma anche favorire in concreto un'ottimale applicazione della disciplina di cui al GDPR.

Il Garante, anzitutto, riconosce la necessità «che, nella descrizione dei trattamenti, siano puntualmente indicate le logiche algoritmiche utilizzate al fine di "generare" i dati e i servizi attraverso i suddetti sistemi di IA, le metriche utilizzate per addestrare il modello e valutare la qualità del modello di analisi adottato, le verifiche svolte per rilevare la presenza di eventuali bias, le misure correttive eventualmente adottate, le misure idonee a verificare, anche a posteriori, le operazioni eseguite da ciascun soggetto autorizzato e i rischi insiti nelle analisi deterministiche e stocastiche»[34].

Nella stessa sede, sempre guardando all'intersezione tra intelligenza artificiale e vigente disciplina in materia di *data protection*, l'Autorità chiarisce in modo ancor più esplicito la cogente imprescindibilità di andare oltre la piena osservanza di quanto sancito *expressis verbis* nel Regolamento generale sulla protezione dei dati, dovendosi informare gli interessati «*non solo in merito agli elementi di cui ai richiamati artt. 13 e 14 del Regolamento* ma anche evidenziando […] se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, nell'ambito dei servizi sanitari, rappresentando le logiche e le caratteristiche di elaborazione dei dati», indicando altresì eventuali specifici obblighi, responsabilità

31. Article 29 Data Protection Working Party 2014.
32. *Ex multis*, cfr. Consiglio di Stato, VI sez., sentenza n. 1206/2021.
33. Autorità Garante per la protezione dei dati personali 2023; il testo, elaborato dall'Autorità nel mese di settembre 2023, è stato pubblicato, in quello successivo, sul sito istituzionale.
34. *Ibidem*.

e benefici correlati all'utilizzo di sistemi di intelligenza artificiale[35].

Da tali approdi ermeneutici del Garante sembrano pertanto potersi desumere utili considerazioni che, andando oltre lo specifico ambito cui il "decalogo" intende riferirsi, non possono non interpellare il mondo delle imprese e, segnatamente, quanto concerne l'adeguatezza degli assetti.

3.2. ...alla sicurezza informatica

Non meno rilevanti, inoltre, risultano i profili di *cybersecurity* nell'ambito dell'intelligenza artificiale[36], anch'essi pregni di rilevanza giuridica, e che meriterebbero una crescente attenzione e maggiori investimenti, *a fortiori* considerata la perfettibile adozione di presidi tecnico-informatici in ambito societario, in special modo da parte delle PMI.

L'approccio *risk based* – imperniato sul principio di *accountability*, che pervade il GDPR[37] e non risulta affatto alieno all'AI Act – contempla anche l'esigenza di non sottovalutare gli ulteriori legami tra sicurezza informatica e trattamento dei dati personali.

Saranno infatti il titolare e l'eventuale responsabile del trattamento a mettere in atto – anche per quei trattamenti che prevedono il ricorso a sistemi di intelligenza artificiale – delle «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio», determinandone *ex ante* l'adeguatezza «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche»[38].

Non solo misure tecnico-informatiche, dunque, ma anche misure organizzative, che tengano conto della singolare rilevanza del "fattore umano" anche nello specifico ambito della sicurezza informatica[39] e che possano in modo adeguato prevenire – e gestire – eventuali violazioni dei dati personali.

A tali considerazioni, si aggiunga, pur senza pretese di completezza, il riferimento all'applicabilità – a specifiche realtà societarie – di più stringenti vincoli normativi, principalmente di matrice unionale.

È questo il caso, in particolare, della direttiva (UE) n. 2022/2555 (meglio nota come direttiva NIS 2)[40], il cui ambito di applicazione, a mente dell'art. 2, par. 1, esula dal novero dei soli soggetti pubblici, ricomprendendo anche gli enti privati «delle tipologie di cui all'allegato I o II"[41] che integrano o superano i requisiti dimensionali propri delle medie imprese e «che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione».

La disciplina della NIS 2 trova altresì applicazione, in talune tassative ipotesi previste *ex lege*, anche in assenza del superamento dei massimali

35. *Ibidem* (corsivo dell'Autore).
36. Anche la rilevanza di tali profili è riconosciuta a livello sovranazionale. Per tutti, sia sufficiente il riferimento a quanto stabilito in OECD 2024. Si tratta della raccomandazione dell'OCSE dedicata all'intelligenza artificiale, adottata il 22 maggio 2019 e recentemente modificata il giorno 8 novembre 2023 e, da ultimo, il 3 maggio 2024 – in cui emergono significativi riferimenti ai principi di *robustness*, *security and safety*. A tale raccomandazione hanno aderito, tra gli altri, gli Stati Uniti d'America e l'Italia.
37. *Ex multis*, cfr. Colapietro–Iannuzzi 2017, p. 106.
38. A mente dell'art. 32, par. 1, GDPR.
39. *Ex multis*, cfr. Sotira 2020 e Fantini 2008, p. 422.
40. Si tratta della direttiva (UE) n. 2022/2555 del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.
41. Gli allegati I e II enumerano rispettivamente i settori ad alta criticità e "altri settori critici", ulteriormente articolati in sottosettori e specifici tipi di soggetti. A titolo meramente indicativo, tra i settori contemplati nel primo allegato, figurano energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario ed infrastrutture digitali; nel secondo, invece, sono ricompresi servizi postali e di corriere, fabbricazione, produzione e distribuzione di sostanze chimiche, produzione, trasformazione e distribuzione di alimenti, fornitura di servizi digitali, ricerca.

per le medie imprese di cui alla Raccomandazione 2003/361/CE [42].

Per quanto maggiormente interessa in questa sede, tra i punti salienti della disciplina, come anticipato applicabile anche a determinate realtà societarie, emerge il capo IV (recante *Misure di gestione del rischio di cibersicurezza e obblighi di segnalazione*) e, in particolare, gli artt. 20 e 21, rubricati rispettivamente *Governance* e *Misure di gestione dei rischi di cibersicurezza*.

In relazione a queste ultime, secondo uno schema non dissimile da quello caratterizzante l'art. 32 GDPR, si prevede che «i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi»[43].

4. Alcuni spunti circa l'adeguatezza degli assetti digitali

Le sintetiche considerazioni sinora illustrate – pur senza pretesa di esaustività – mirano a gettare ulteriore luce sui profili problematici, se non di vera e propria criticità, emergenti in ambito societario per quanto concerne la concreta gestione delle tecnologie digitali.

In particolare, prima di evidenziare come il ricorso a sistemi di intelligenza artificiale possa rientrare tra quelli che la dottrina considera "rischi tecnologici d'impresa"[44], le esemplificazioni proposte evidenziano come la debita presa in considerazione – servendosi funzionalmente di una opportuna opera ricognitiva – di discipline settoriali e caratterizzate da una significativa portata innovativa non possa prescindere da una visione d'insieme, che – come si è avuto modo sinteticamente di evidenziare – sia in grado di fare emergere anche la rilevanza trasversale di quanto pertiene all'adozione di misure tecniche e organizzative adeguate, così come alla previa valutazione ed alla continua gestione dei rischi.

Sotto quest'ultimo profilo, va altresì apprezzata in concreto la crescente importanza riconosciuta al vigente quadro normativo in materia di *data protection*, come evidenziata dalla recente dottrina che, con gli occhi del giurista, si è interessata all'ambito del *risk management*[45].

D'altra parte, le nuove sfide poste (anche) dall'intelligenza artificiale invitano l'interprete, già da oggi, a non procedere per compartimenti stagni nella gestione dei rischi, non essendo più sufficiente la mera attribuzione di autonoma dignità e rilevanza ad una specifica disciplina, senza vagliare le confluenze interdisciplinari tra vari ambiti specifici.

Risulta altresì improcrastinabile l'esigenza di un effettivo superamento dell'approccio formalistico talora emergente in sede di *compliance* normativa[46], sempre più inadatto soprattutto nei contesti ad elevata innovazione tecnologica. Anche in questo caso, interessanti spunti possono essere attinti dall'ambito del *risk management*, laddove scienze giuridiche e aziendalistiche trovano costruttivi e non del tutto esplorati spazi di dialogo e di reciproca fruttuosa influenza.

Se è vero che «la gestione del rischio rappresenta oggi l'architrave di una buona *corporate governance*»[47] – come peraltro confermato all'interno dei Principi di *Corporate Governance* G20/OCSE

42. Cfr. art. 2, parr. 2, 3 e 4, direttiva NIS 2.
43. Così l'art. 21, par. 1, della direttiva NIS 2, ove si statuisce peraltro che l'adozione di tali misure debba avvenire «tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico».
44. Si veda, in proposito, Schneider 2023, pp. 32-33.
45. Cfr. Veronese 2019, p. 275 ss.
46. In senso sostanzialmente conforme, si rimanda, per tutti, a Vernero–Parena–Artusi 2019, p. 33.
47. Così Montalenti 2019, p. 17.

di settembre 2023[48] – tale affermazione può valere, *a fortiori*, nel contesto della *Corptech governance* e, quindi, ai fini di una strutturazione adeguata degli assetti digitali societari.

Il tutto senza dimenticare la rilevanza di quanto sinora affermato all'interno del più ampio contesto degli assetti organizzativi, amministrativi e contabili che, a mente dell'art. 2086, comma 2, c.c., «l'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire», avendo peraltro cura che siano in concreto adeguati «alla natura e alle dimensioni dell'impresa»[49].

Tali assetti, inoltre, vanno considerati non solamente nell'ottica funzionale alla rilevazione tempestiva della crisi d'impresa, come pure attualmente sancito *expressis verbis* nel prosieguo del medesimo art. 2086, comma 2, c.c.[50], ma quale obbligo di più ampio respiro, intimamente connaturato alla corretta gestione dell'impresa collettiva, in modo non dissimile dalla previsione codicistica di cui all'art. 2381 c.c.[51].

In argomento, risulta imprescindibile sottolineare come l'adozione di sistemi di intelligenza artificiale e, segnatamente, l'inclusione dei medesimi negli assetti organizzativi di una società, travalichi gli obblighi di portata generale, evidenziati nei paragrafi precedenti, comportando invero il necessario riferimento a norme fondamentali del diritto societario.

Sul punto, l'adeguatezza degli assetti, introdotta espressamente a livello codicistico con la riforma del diritto societario del 2003, viene riconosciuta quale «elemento qualificante dei principi di corretta gestione»[52] e sorta di declinazione dei medesimi[53], come emerge anche *ex* art. 2403 c.c., ove viene attribuito dal legislatore al collegio sindacale il dovere di vigilanza, fra l'altro, «sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato».

Si tratta di una clausola generale, la cui piena osservanza può in concreto comprimere l'autonomia privata, così come la libertà di iniziativa economica[54], laddove le scelte dell'organo gestorio devono risultare finalisticamente orientate anche all'adeguatezza degli assetti.

Se, come efficacemente sintetizzato da autorevole dottrina, la predisposizione – e successiva gestione – di adeguati assetti può essere considerata come «il dovere organizzativo di più elevato grado»[55], il ricorso a sistemi di intelligenza artificiale, che pure implica una idonea procedimentalizzazione, contribuisce a far emergere ulteriormente la crescente ed «accentuata complessità e rischiosità delle scelte manageriali»[56].

Ciò posto, nel considerare le implicazioni del ricorso a sistemi di intelligenza artificiale in ambito societario, risulta necessario riconoscere l'imprescindibilità, prima ancora di una corretta gestione dei "rischi tecnologici in senso stretto", ontologicamente correlati ad una specifica tecnologia, di quel "rischio prevalentemente strategico" che si radica ogniqualvolta quest'ultima venga introdotta nel contesto dell'esercizio di attività d'impresa[57].

5. Il ruolo della *Corporate Digital Responsibility*

Emerge quindi come un approccio orientato al *risk management* – più precisamente, alla gestione integrata del rischio propria dell'*Enterprise Risk*

48. Cfr. OECD 2023. Si noti come, all'interno di tale documento, venga auspicata, a supporto dell'organo gestorio, la costituzione di gruppi di esperti, secondo criteri di flessibilità e proporzionalità alle esigenze specifiche.
49. Per tutti, in argomento, si veda Cavaliere 2019, p. 1943 ss.
50. Cfr. Panzani 2020, p. 656.
51. *Ex multis*, cfr. Bruno 2020, p. 51.
52. Così Montalenti 2016, p. 6.
53. *Ex multis*, cfr. Irrera 2005, p. 69.
54. Cfr. Meruzzi 2016, pp. 43-44 e 53-54.
55. Irrera 2005, p. 81.
56. Nappo 2020, p. 90.
57. Schneider 2023, p. 32.

Management[58] –, corroborato da una corretta e non parcellizzata visione e gestione delle varie tecnologie digitali utilizzate in una specifica realtà societaria, possa far sì che non vadano perduti frammenti giuridicamente rilevanti anche ai fini dell'osservanza del principio generale di corretta amministrazione.

In altre parole, ciò potrebbe massimizzare anche i benefici che possono derivare da un ricorso al digitale che non sia solo formalmente *compliant*, ma anche sostanziale ed efficiente applicazione di quelle regole di condotta che l'organo gestorio dovrà sempre più tenere in considerazione – sebbene caratterizzate da una formulazione generica o, talora, priva di natura cogente – nelle loro concrete declinazioni.

Ampliare lo sguardo, considerare il rischio come un *upside risk*, foriero anche di opportunità, adottare procedure interne che, partendo da una mappatura delle tecnologie e dalla definizione dei ruoli, possano concretamente incidere nella predisposizione di assetti digitali adeguati, soprattutto di natura organizzativa, costituiscono condotte non solo utili, ma anche doverose nel contesto dell'ordinario esercizio di attività d'impresa.

Le molteplici peculiarità dell'intelligenza artificiale giuridicamente rilevanti in ambito societario, considerate *una cum* i recenti approcci del *risk management*, come evidenziati dalla più autorevole dottrina, possono altresì suggerire di attenzionare l'ambito della *Corporate Digital Responsibility* che, in argomento, può giocare un ruolo molto rilevante.

Essa è stata tratteggiata anzitutto come una "sottocategoria" della *Corporate Social Responsibility* nei primi recepimenti ad opera della dottrina italiana, che ne ha evidenziato il legame con l'ambito tecnologico che maggiormente interessa in questa sede e, in particolare, ai «coessenziali profili di responsabilità digitale di quelle società che includono nei propri assetti tecnologie di intelligenza artificiale»[59]. Elementi di responsabilità sociale d'impresa vengono altresì evocati con particolare riguardo alla correttezza della strutturazione e dell'utilizzo delle "tecnologie societarie", peraltro «avendo attento riguardo ai possibili impatti sociali e ambientali delle stesse»[60] .

Ciò posto, risulta opportuno non circoscrivere in via esclusiva l'ambito di pertinenza della *Corporate Digital Responsibility* ad una determinata tecnologia, onde evitare di vanificare quei benefici di singolare rilevanza informatico-giuridica che possono derivare significativamente solo da un qualificato sguardo d'insieme relativo agli assetti digitali di una determinata realtà societaria.

Inoltre, ulteriori approcci dottrinali confermano che la *Corporate Digital Responsibility*, seppur caratterizzata da significative affinità con quanto pertiene alla sostenibilità sociale, sia caratterizzata da una autonoma rilevanza[61]: in argomento, la dottrina tedesca si è spinta a considerare quanto concerne il ricorso agli strumenti digitali, nel contesto dell'esercizio di attività d'impresa, un vero e proprio settore della *Corporate Responsibility*[62].

Tali considerazioni circa la crescente opportunità di sposare un inquadramento tassonomico della *Corporate Digital Responsibility* che sia in grado di evidenziarne l'autonoma rilevanza e, al contempo, di coglierne i profili dinamici[63], intendono costituire uno stimolo ad ulteriori studi in materia, nella consapevolezza che la responsabilità digitale d'impresa rappresenta uno stimolante crogiolo, punto d'incontro tra le competenze interdisciplinari degli esperti e le esigenze degli amministratori, in grado di favorire la migliore gestione delle multiformi sfide del digitale in ambito societario, con riguardo anche all'adozione di sistemi di intelligenza artificiale.

In argomento, l'apporto del giurista informatico può giocare un ruolo determinante nel coadiuvare

58. Un approccio integrato (e interdisciplinare) specificamente riferito ai rischi dell'intelligenza artificiale si riscontra nell'*Integrated AI-Risk Management* (IARM), «processo aziendale di risk management autonomo […] sia pure sempre inserito in quello più generale di gestione del rischio d'impresa» proposto e descritto in Cerrato–Culasso–Crocco 2023, p. 319 ss.

59. Schneider 2022, p. 720.

60. *Ibidem*.

61. A titolo esemplificativo, si veda Lobschat–Mueller–Eggers et al. 2021, p. 876.

62. Dörr 2021, pp. XIII e 2.

63. *Ivi*, pp. 5 e 35 ss.

l'approfondimento concernente i rischi tecnologici d'impresa, stimolando un'analisi del rapporto tra diritto societario e tecnologie digitali improntata ad un approccio olistico e che sia in grado, al contempo, di far tesoro dei rilevanti spunti desumibili dai più recenti approdi della dottrina.

Riferimenti bibliografici

N. Abriani, G. Schneider (2021), *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, il Mulino, 2021

Article 29 Data Protection Working Party (2014), *Opinion 05/2014 on Anonymisation Techniques*, 2014

Autorità Garante per la protezione dei dati personali (2023), *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale*, 2023

M. Bianchini, G. Gasparri, G. Resta et al. (a cura di) (2022), *Gli sviluppi tecnologici del diritto societario*, Quaderni giuridici CONSOB, n. 23, 2022

R. Borruso, S. Russo, C. Tiberi (2009), *L'informatica per il giurista. Dal bit a Internet*, Giuffrè, 2009

S. Bruno (2020), *Cambiamento climatico e organizzazione delle società di capitali a seguito del nuovo testo dell'art. 2086 c.c.*, in "Banca, Impresa, Società", 2020, n. 1

T. Cavaliere (2019), *Codice della crisi d'impresa e dell'insolvenza. Le modificazioni del Codice civile*, in "Giurisprudenza Italiana", 2019, n. 8-9

S.A. Cerrato, F. Culasso, E. Crocco (2023), *"Handle with care". Per una governance dell'intelligenza artificiale nell'impresa: rischi, tecniche di gestione, assetti cibernetici*, in N. Abriani e R. Costi (a cura di), "Diritto societario, digitalizzazione e intelligenza artificiale. In ricordo di Agostino Gambino", Giuffrè, 2023

S.A. Cerrato (a cura di) (2019), *Impresa e rischio. Profili giuridici del* risk management, Giappichelli, 2019

C. Ciccia Romito (2021), *Il GDPR nella micro, piccola e media impresa*, Giuffrè, 2021

R.M. Colangelo (2023), *Informatica giuridica e impresa: nuove prospettive di Corporate Digital Responsibility*, in "Rivista elettronica di Diritto, Economia, Management", 2023, n. 2

C. Colapietro, A. Iannuzzi (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano e C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017

S. Dörr (2021), *Corporate Digital Responsibility. Managing Corporate Responsibility and Sustainability in the Digital Age*, Springer Verlag, 2021

L. Enriques, D.A. Zetzsche (2019), *Corporate Technologies and the Tech Nirvana Fallacy*, ECGI, Law Working Paper n. 457/2019

European Commission (2023-a), *Report on the state of the Digital Decade 2023*, 2023

European Commission (2023-b), *Report on the state of the Digital Decade 2023. Annex Italy*, 2023

M. Fantini (2008), Phishing: *strategie operative dell'inganno*, in "Diritto dell'Internet", 2008, n. 4

M. Irrera (2005), *Assetti organizzativi adeguati e governo delle società di capitali*, Giuffrè, 2005

ISTAT (2023), *Rilevazione sulle tecnologie dell'informazione e della comunicazione (Ict)*, 2023

P. Liberanome (2022), *Criptoarte e nuove sfide alla tutela dei diritti autorali*, in "I Contratti", 2022, n. 1

L. Lobschat, B. Mueller, F. Eggers et al. (2021), *Corporate digital responsibilty*, in "Journal of Business Research", 2021, n. 122

D. Matricano (2020), *Fare impresa nell'era digitale. Analisi teoriche e riflessioni critiche su un processo business-driven e technology-enabled*, Giappichelli, 2020

A. Micozzi (a cura di) (2024), *L'attivazione imprenditoriale in Italia. Rapporto GEM 2023-2024*, FrancoAngeli, 2024

L. Miotto (2023), *Organizzazione d'impresa e gestione dei dati personali. Il rischio di non compliance nelle catene di fornitura*, Giappichelli, 2023

P. Montalenti (2019), *Introduzione*, in S.A. Cerrato (a cura di), "Impresa e rischio. Profili giuridici del *risk management*", Giappichelli, 2019

P. Montalenti (2016), *I principi di corretta amministrazione*, in M. Irrera (a cura di), "Assetti adeguati e modelli organizzativi nella *corporate governance* delle società di capitali", Zanichelli, 2016

G.D. Mosco (2019), *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in "Analisi Giuridica dell'Economia", 2019, n. 1

F. Nappo (2020), *Aziende e intelligenza artificiale. Prime riflessioni critiche*, FrancoAngeli, 2020

OECD (2024), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2024

OECD (2023), *G20/OECD Principles of Corporate Governance 2023*, OECD Publishing, 2023

L. Panzani (2020), *La disciplina degli assetti ai fini della rilevazione della crisi, con particolare riferimento alla s.r.l.*, in M. Irrera (a cura di), "La società a responsabilità limitata: un modello transtipico alla prova del Codice della Crisi. Studi in onore di Oreste Cagnasso", Giappichelli, 2020

F. Pascucci (2017), *Lo stato della "trasformazione digitale" nelle PMI italiane e sfide emergenti*, in F. Pascucci, V. Temperini (a cura di), "Trasformazione digitale e sviluppo delle PMI. Approcci strategici e strumenti operativi", Giappichelli, 2017

M. Pietrangelo (2007), *La società dell'informazione tra realtà e norma*, Giuffrè, 2007

R. Rolli (2018), *Il Diritto privato nella società 4.0*, Wolters Kluwer - Cedam, 2018

G. Scarchillo (2019), Corporate Governance *e Intelligenza Artificiale*, in "La nuova giurisprudenza civile commentata", 2019, n. 4

G. Schneider (2023), *La proposta di Regolamento sull'intelligenza artificiale: le possibili ripercussioni sull'attività di impresa*, in M. Rescigno (a cura di), "L'impresa nell'era dell'intelligenza artificiale: un'evoluzione tranquilla o nulla sarà più lo stesso?", Giuffrè, 2023

G. Schneider (2022), *Intelligenza artificiale, governance societaria e responsabilità sociale d'impresa: rischi e opportunità. Prima parte*, in "La nuova giurisprudenza civile commentata", 2022, n. 3

M. Soffientini (2023), *I sistemi di videosorveglianza intelligenti*, in M. Soffientini (a cura di), "Gli adempimenti privacy per i sistemi di videosorveglianza", Giuffrè, 2023

N. Sotira (a cura di) (2020), *Il fattore umano nella cyber security. Valori e strategie da costruire insieme*, FrancoAngeli, 2020

Unioncamere – ANPAL (2023), *Sistema Informativo Excelsior (2023), Nuove imprese. Caratteristiche e fabbisogni professionali delle nuove imprese. Indagine 2023*, 2023

P. Vernero, B. Parena, M.F. Artusi (2019), Risk management *e modelli organizzativi*, in S.A. Cerrato (a cura di) "Impresa e rischio. Profili giuridici del *risk management*", Giappichelli, 2019

B. Veronese (2019), *Privacy 4.0: oneri e strategie per le PMI*, in S.A. Cerrato (a cura di) "Impresa e rischio. Profili giuridici del *risk management*", Giappichelli, 2019