Comparative Law Review

2024 – Vol. 15 n. 3

ISSN:2038 - 8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Department of Law - University of Perugia
Via Pascoli, 33 - 06123 Perugia (PG) - Telephone 075.5852437
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE LAW REVIEW

VOL. 15/3 - 2024

L'ASPETTATIVA DI PRIVACY DEL LAVORATORE: PROSPETTIVE DI DIRITTO COMPARATO[1*]

Federica Giovanella

SOMMARIO:
I. LA "RAGIONEVOLE ASPETTATIVA DI PRIVACY"; II. LO SCENARIO STATUNITENSE; 2.1 IL CONTESTO DI LAVORO PUBBLICO; 2.2 IL CONTESTO DI LAVORO PRIVATO; III. L'ESPERIENZA CANADESE; IV. GLI INTERVENTI DELLA CORTE EDU; V. UN CONFRONTO FRA GLI APPROCCI SOTTO LA LENTE "ITALIANA"; VI. CONCLUSIONI

Il contributo analizza il concetto di ragionevole aspettativa di privacy nel contesto lavorativo, ponendo a confronto la più rilevante giurisprudenza delle corti statunitensi e canadesi e della Corte Europea dei Diritti dell'Uomo. L'indagine si concentra sulla privacy nell'utilizzo degli strumenti di lavoro e dimostra la centralità delle informative adottate dai datori di lavoro in ciascuno dei contesti. La comparazione evidenzia un approccio molto distante fra Stati Uniti da un lato e Canada e Corte EDU dall'altro e dimostra come, pur in assenza di qualunque riferimento al concetto di ragionevole aspettativa di privacy nel contesto italiano, la giurisprudenza interna in materia di controlli difensivi possa essere considerato un equivalente funzionale.

The paper analyzes the concept of reasonable expectation of privacy in the employment context, comparing the most relevant case law from the U.S. and Canadian courts and the European Court of Human Rights. The investigation focuses on privacy in the use of work tools and demonstrates the centrality of the written policies adopted by employers in each of the contexts. The comparison shows a very distant approach between the United States on the one hand and Canada and the ECtHR on the other; it also and reveals how, even in the absence of any reference to the concept of reasonable expectation of privacy in the Italian context, domestic jurisprudence on defensive controls might be considered as a functional equivalent of it.

Keywords: ragionevole aspettativa di privacy/reasonable expectation of privacy – privacy dei lavoratori/workers' privacy – Corte Europea dei Diritti dell'Uomo/European Court of Human Rights – Diritto comparato del lavoro/Comparative labor law – Protezione dei dati personali/ Personal data protection

I. LA "RAGIONEVOLE ASPETTATIVA DI PRIVACY"

Le problematiche relative alla sorveglianza del lavoratore, certamente non nuove, si intensificano e si acuiscono con l'utilizzo delle moderne tecnologie, che come noto permeano la vita lavorativa di ciascuno.

Le controversie nascenti dal sempreverde scontro fra esigenze datoriali e diritti dei dipendenti sfociano in molteplici sentenze, spesso connotate da una certa rilevanza anche per il fatto che sono emanate da Corti in posizioni apicali.

* Questo articolo è il risultato di un lavoro che ha potuto giovarsi di consigli e suggerimenti di diversi colleghi. Desidero ringraziare i partecipanti agli eventi «Lavoro e Diritti nella Rivoluzione di Internet», tenutosi presso l'Università Ca' Foscari di Venezia il 13 e 14 gennaio 2022, e «Gikii 2023», svoltosi a Utrecht nei giorni 7 e 8 settembre 2023. Il contributo si colloca all'interno del PRIN PRIN2017EC9CPX "Dis/Connection: Labor and Rights in the Internet Revolution", nonché dentro al progetto "Tecnologie digitali, diritto comparato e 'Brussels Effect'" finanziato dal Dipartimento di Scienze Giuridiche dell'Università di Udine. Ringrazio infine gli anonomi *reviewers* che hanno effettuato il referaggio di questo articolo.

Il presente contributo intende concentrarsi sulla privacy e la protezione di dati personali del lavoratore, rifacendosi più precisamente al concetto di "reasonable expectation of privacy" in una prospettiva comparatistica che contempla gli ordinamenti statunitense e canadese, raffrontandoli all'approccio seguito dalla Corte Europea dei Diritti dell'Uomo. L'analisi parte da alcune importanti decisioni adottate dalle Corti di questi sistemi e indaga appunto la ragionevole aspettativa di riservatezza nutrita dal lavoratore, nella consapevolezza che solo quando al lavoratore sia riconosciuto un certo grado di privacy, il giudice può procedere a bilanciare questo diritto del dipendente con gli interessi del datore di lavoro.

L'aspettativa di riservatezza, concetto pressoché sconosciuto all'ordinamento italiano[2], è invece condiviso dagli ordinamenti nordamericani e regolarmente applicato dalla Corte EDU. Non si tratta di una nozione confinata all'ambito lavorativo; al contrario, essa si è sviluppata al di fuori di tale contesto per poi confluirvi. Si suole ricondurre tale nozione al caso *Katz v. US* deciso dalla Corte Suprema nel 1967[3]. Charles Katz utilizzava delle cabine telefoniche per effettuare scommesse illecite; sulla base di fondati sospetti, l'FBI installò all'esterno di una cabina telefonica pubblica un c.d. "telephone bug" che permetteva di monitorare le conversazioni, dalle quali fu possibile evincere che in effetti Katz stava commettendo degli illeciti e fu pertanto imputato. Egli cercò di far sopprimere le prove perché raccolte in assenza di un mandato e, dunque, in violazione del 4° emendamento della Costituzione americana[4].

Il caso giunse davanti alla Corte Suprema che, ribaltando il risultato dei primi due gradi di giudizio[5] e rivedendo il proprio orientamento[6], ritenne che le operazioni di ascolto da parte del governo avessero violato la privacy che il ricorrente poteva ragionevolmente attendersi e costituivano "search and seizure" ai sensi del 4° emendamento. Tale emendamento non poteva essere limitato alla protezione degli oggetti tangibili, ma doveva essere esteso anche alle espressioni orali[7].

Il lascito più famoso di questa decisione è il c.d. "reasonable expectation of privacy test" proposto da Justice Harlan nella sua opinione concorrente. Nelle parole del giudice "the rule that has emerged from prior decisions is that there is a twofold requirement, first that

[2] Da una ricerca nelle banche dati giurisprudenziali, questa espressione sembra essere stata utilizzata esclusivamente nella sentenza Cass. pen, 28.9.2010, n. 37751 in Cass. pen. 2011, 10, 3512, dunque in un contesto diverso da quello qui di interesse.

[3] 389 U.S. 347 (1967).

[4] Come noto, tale emendamento tutela i cittadini contro perquisizioni e sequestri irragionevoli e prescrive che essi debbano essere preceduti da un mandato che descriva i luoghi da perquisire e le persone o le cose da sequestrare.

[5] *Katz v. U.S. (Appeal),* 369 F.2d 130 (9th Cir. 1967).

[6] Il riferimento è principalmente a *Olmstead v. U.S.,* 277 U.S. 438 (1928) e *Goldman v. U.S.*, 316 U.S. 129 (1942). In *Olmstead v. United States*, attraverso una *dissenting opinion*, Justice Braindeis ritenne che il Quarto Emendamento dovesse essere applicato oltre i confini della mera violazione di domicilio, per considerare anche la tutela delle situazioni immateriali, del "right to be let alone", quale diritto fondamentale dell'uomo civilizzato; v., Olmstead v. United States cit., 478.

[7] "[I]t protects people, rather than places": *Katz v. U.S.*, cit., 351.

a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'"[8].

Calare il concetto di "ragionevole aspettativa di privacy" nel contesto lavorativo significa effettuare un'indagine sulle informazioni a disposizione del lavoratore riguardo al luogo di lavoro e agli strumenti che utilizza al fine di comprendere se e in che termini egli potesse nutrire una qualche aspettativa di riservatezza sui medesimi.

In quest'ottica, il presente contributo intende analizzare la più rilevante giurisprudenza delle corti statunitensi e canadesi e della Corte Europea dei Diritti dell'Uomo, concentrandosi sulle decisioni che hanno a oggetto la riservatezza relativa all'uso degli strumenti lavorativi. Da un punto di vista metodologico, la scelta di fare riferimento a quest'ultima è dovuta all'assenza a livello di Unione Europea e, dunque, di Corte di Giustizia, di pronunce sufficienti per poter parlare di indirizzi o orientamenti dominanti[9].

Al contempo, una comparazione con il solo sistema italiano risulterebbe poco significativa per due motivi: in primo luogo per l'irriducibilità dell'intero contesto europeo a un unico sistema; in secondo luogo perché il nostro sistema giuridico non considera la figura della ragionevole aspettativa di privacy. Le ragioni per cui il sistema italiano non contempla, almeno attualmente, una simile figura sono probabilmente molteplici. Una di esse è sicuramente l'approccio diverso che il nostro sistema adotta rispetto ai sistemi nordamericani, approccio che certamente è anche un precipitato dell'appartenenza al sistema euro-unitario. Volendo approssimare e generalizzando, il sistema italiano di protezione dei dati personali ragiona in termini "binari": un comportamento o è lecito o non lo è. Non c'è spazio per invocare un'aspettativa. Al contempo ciò non vuole significare che non vi siano degli equivalenti funzionali. Come si avrà modo di accennare in chiusura di questo lavoro, parte delle funzioni esercitate dalla ragionevole aspettativa di privacy sono ricoperte in Italia dal noto fenomeno dei c.d. "controlli difensivi".

Ai fini comparatistici, il presente contributo si concentrerà sui parametri che le corti considerano per determinare l'aspettativa di privacy del lavoratore nel caso concreto, tenendo in considerazione anche le differenti valutazioni effettuate dagli organi giudicanti in relazione al diverso contesto lavorativo (es. pubblico vs. privato). Si analizzerà la giurisprudenza rilevante dei sistemi nordamericani (parr. 2 e 3) e quella della Corte

[8] *Katz v. U.S.*, cit., 362. Nella sua opinione concorrente Justice Harlan riconobbe il potenziale delle tecnologie cui era associata un'intrusività precedentemente sconosciuta, in grado di ostacolare una ragionevole aspettativa di privacy negli stessi termini di un'intrusione fisica e materiale nella proprietà altrui.

[9] Non mancano infatti decisioni relative alla riservatezza del lavoratore, ma nessuna di esse si concentra sui temi di cui al presente scritto. Si v. per esempio: CGUE, 20 maggio 2003, Cause riunite C- 465/00, *Rechnungshof c. Österreichischer Rundfunk* e altri; C-138/01, *Christa Neukomm* e C-139/01, *Joseph Lauermann c. Österreichischer Rundfunk*. V. in materia M. OTTO, *The Right to Privacy in Employment. In Search of the European Model of Protection*, *European Labor Law Journal*, 2015, 343, spec. 356. Si v. anche D. MANGAN, *Guidance from the EU Courts: Privacy in the Workplace*, in C. PISANO, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, 2022, 43 ss. Sebbene manchi una giurisprudenza sui temi qui considerati, l'Unione Europea regola in vario modo il diritto alla privacy dei lavoratori. Si rinvia per approfondimenti a: M. FREEDLAND, *Data Protection and Employment in the European Union: An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and Its Member States*, Oxford, 1999; F.H.R. HENDRICKX, *Employment privacy law in the European Union: monitoring and surveillance*, Anversa, 2002; IDEM, *Protection of workers' personal data in the European Union Two studies 1. Study on the protection of workers' personal data in the European Union: general issues and sensitive data. 2. Study on the protection of workers' personal data in the European Union: surveillance and monitoring at work*, European Commission, 2003; M. OTTO, *The Right to Privacy in Employment. A Comparative Analysis*, Portland, 2016.

Europea dei Diritti dell'Uomo (par. 4), per poi procedere a una comparazione anche alla luce del sistema italiano (par. 5), concludendo con delle brevi riflessioni (par. 6).

II. LO SCENARIO STATUNITENSE

Il sistema giuridico che sembra aver dato i natali al concetto stesso di privacy[10] presenta da sempre una disciplina a tutela della riservatezza e della protezione dei dati personali frammentata e disomogenea, affidata a un elevato numero di normative che in genere si concentrano solo su determinati settori[11] oppure rispondono a esigenze che si potrebbero definire emergenziali[12].

A fianco di queste normative si pongono alcune figure di *torts*[13], le regolamentazioni statati[14], e una protezione più ampia ricondotta alla Costituzione. Le regolamentazioni statali sono connotate a loro volta da una certa settorialità, anche se rivolte sia al contesto pubblico sia a quello privato[15], inclusi alcuni interventi specifici a tutela della privacy del lavoratore da parte di taluni Stati[16]. Di recente alcuni Stati hanno parzialmente riformato il loro impianto di tutela introducendo normative ampie e tendenzialmente omnicomprensive[17], in risposta all'adozione del *General Data Protection Regulation* da parte

[10] L'immancabile citazione è per S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

[11] A titolo d'esempio si considerino le normative che fanno riferimento alla privacy "finanziaria" (Right to Financial Privacy Act – 1978); a quella delle comunicazioni elettroniche (Electronic Communications Privacy Act – 1986); alla privacy degli utenti contro le vendite telefoniche (Telephone Consumer Protection Act – 1988); alla privacy dei guidatori (Driver's Privacy Protection Act – 1994); alla protezione dal c.d. "spam" via *e-mail* (CAN-SPAM Act – 2003).

[12] Tra questi sono particolarmente noti il Video Privacy Protection Act (1988), ancora il Driver's Privacy Protection Act (1994), lo US PATRIOT-Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act – 2001), ma già il Privacy Act del 1974, in risposta al c.d. "Scandalo Watergate", v. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, New York, 2021, 685 ss.

[13] Alcune di queste figure provengono dal *common law* (*breach of confidentiality, defamation, infliction of emotional distress*), mentre altre sono state teorizzate da William Prosser (cf. W. PROSSER, *Privacy*, 48 California Law Review 383 (1960)) e successivamente inserite nel Restatement (Second) of Torts § 652. V. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, cit., 32 ss.

[14] Ciascuno stato ha promulgato leggi di protezione della privacy sotto diversi profili, sia nel settore privato che pubblico. Cf. D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, cit., 39-40.

[15] D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, cit., 39.

[16] V. Delaware Labor Code, Title 19 § 705; Connecticut General Statutes §31-48d; California Labor Code § 435; West Virginia Code § 21-3-20; Rhode Island General Laws §28-6.12-1. Sul punto si consideri L. DETERMANN, R. SPRAGUE, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, *26 Berkeley Tech. L.J. 979* (2011), 993 ss.; A. EICHELBERGER, *Note: Global Employee Privacy: A Case Study on the Minefiled of Employee Privacy Rights in the EU, USA, and KSA*, 31 Indiana International & Comparative Law Review 177 (2021), 182.

[17] Si vedano a titolo d'esempio i provvedimenti: "California Privacy Rights Act (CPRA)" del 2020; "California Consumer Privacy Act (CCPA)" del 2018, emendato dal "California Privacy Rights Act" del 2023; "Colorado Privacy Act (CPA)" del 2021; "Virginia Consumer Data Protection Act" del 2021; "Connecticut Consumer Data Protection Act" del 2022; "Utah Consumer Data Protection Act" del 2022; "Indiana Consumer Data Protection Act" del 2023; "Texas Data Privacy and Security Act" del 2023; "Tennesee Informamtion Protection Act" del 2023; "New Jersey Data Privacy Act (NJDPA)" del 2024; si veda in generale: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws.

dell'UE [18] e quale tentativo di superare le note difficoltà legate al trasferimento transfrontaliero di dati[19].

Venendo brevemente alla protezione costituzionale a livello federale[20], seppur non esista una previsione che esplicitamente tuteli la privacy, essa è ricondotta a più emendamenti[21]. Già nel 1965 la Corte Suprema aveva ritenuto che nelle "zone di penombra" delle libertà garantite dal Bill of Rights si potesse rinvenire un diritto alla privacy costituzionale[22]. Qualche anno più tardi la stessa corte ammise la protezione anche dell'aspetto informazionale della privacy, riconoscendo un interesse individuale a evitare la divulgazione di fatti personali[23].

Come già brevemente illustrato, l'emendamento che qui maggiormente interessa è il Quarto e nello specifico il concetto di ragionevole aspettativa di privacy. Nonostante tale nozione non sia esente da critiche e difetti[24], essa continua a trovare applicazione anche in casi particolarmente complessi[25], incluse numerose controversie nel contesto lavorativo.

---

[18] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GUUE L119/1, 4.5.2016, p. 1–88.

[19] Sono note le vicende giudiziarie relative ai c.d. casi "Schrems I" (CGUE, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 ottobre 2015) e "Schrems II" (CGUE, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, 16 luglio 2020). Per le implicazioni che queste decisioni hanno avuto e avranno sul trasferimento transfrontaliero di dati, si v. lo studio di I. BROWN, D. KORFF, *Exchanges of Personal Data After the Schrems II Judgment*, 2021, disponibile all'url: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3884896. Attualmente il trasferimento di dati avviene sulla base del c.d. "EU-US Data Privacy Framework", la cui decisione di adeguatezza è stata adottata dalla Commissione UE il 10 luglio 2023.

[20] Si registrano infatti alcuni riconoscimenti del diritto alla privacy anche a livello di costituzioni statali, v. per esempio le costituzioni di Alaska (art. 1, sec. 22), California (art. 1, sec. 1), Florida (art. 1, sec. 23).

[21] Uno fra questi è sicuramente il Primo Emendamento, che viene normalmente invocato quando si tratti di anonimato, in quanto tale emendamento protegge la liberà di espressione. Si v. ad es. la decisione *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995), in cui la Corte Suprema statunitense ritenne incostituzionale una legge dell'Ohio che proibiva la distribuzione di letteratura anonima a sfondo politico.

[22] *Griswold v. Connecticut*, 381 U.S. 479 (1965). Secondo A. WESTIN, *Privacy and Freedom*, cit., 355, in questa sentenza il diritto alla privacy si avvicinava molto alla teorizzazione di Warren e Brandeis. Si vedano in proposito le parole di Justice Black (*Griswold v. Connecticut*, cit., 510).

[23]4 *Whalen v. Roe*, 29 U.S. 589 (1977), 599. Il caso riguardava informazioni sulla prescrizione di medicinali che i medici erano obbligati a trasmettere al Dipartimento di Stato, che li avrebbe conservati nei propri database. Alcuni pazienti e medici, insieme ad associazioni di categoria, impugnarono la legge che introduceva tale obbligo. Sebbene la Corte Suprema non la abrogò, la sentenza assunse rilievo in quanto i giudici ritennero che esistesse un diritto alla protezione dei dati personali, a presidio di due diversi, seppur collegati, interessi: il primo era l'interesse a controllare la divulgazione di informazioni personali e il secondo l'interesse ad essere in grado di compiere determinate scelte personali liberi dall'influenza del Governo. La Corte ritenne che la normativa impugnata non scalfisse questi interessi al punto tale da dover essere abrogata.

[24] V. ad es. R.G. WILKINS, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077, 1089 (1987); G.A. ASHDOWN, *Legitimate Expectation of Privacy*, 34 Vand. L. Rev. 1289 (1981); A. LIBEU, *What is a reasonable expectation of privacy?*, 12 W. St. U. L. Rev. 849 (1985). Si veda anche la critica mossa da Justice Scalia nel famoso caso deciso dalla Corte Suprema *Kyllo v. United States*, 533 U.S. 27, 34 (2001), nonché da R. POSNER, *The Uncertain Protection of Privacy by the Supreme Court*, The Supreme Court Review, 1979, 173, 188, concernente la circolarità dei requisiti del test.

[25] Fra i più recenti casi decisi dalla Corte Suprema: *Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. U.S.*, 138 S. Ct . 2206 (2018), *Torres v. Madrid*, 141 S. Ct. 989 (2021). Sugli ultimi sviluppi della giurisprudenza della *Supreme Court* sul 4° emendamento v. M. TOKSON, *The aftermath of Carpenter: an empirical study of fourth amendment law*, 2018–2021, 135 *Harv. L. Rev.* 1790 (2022).

Al fine di meglio illustrare l'atteggiarsi dell'aspettativa di privacy in tale ambito, è bene differenziare le controversie che vedono contrapporsi un dipendente e un datore di lavoro pubblici dalle controversie che invece coinvolgono attori del settore privato. Si deve infatti premettere che i lavoratori pubblici sono protetti da una serie di interventi legislativi, dal *Privacy Act* del 1974, dalle normative sulle intercettazioni [26], nonché dal Quarto Emendamento, anche se limitatamente. Vi sono poi molte costituzioni statali che proteggono la riservatezza dei dipendenti pubblici[27].

Per quanto riguarda i dipendenti del settore privato, sebbene possano godere di alcune delle protezioni concesse ai loro pari del settore pubblico, non trova applicazione il Quarto Emendamento, né trovano tutela, salvo eccezioni, nelle costituzioni statali[28]. Sono invece applicabili alcuni *Act* in tema di privacy[29], nonché le figure di *privacy torts* derivate dal *common law*, in particolare il *tort* di *intrusion upon seclusion*[30]. A ciò si aggiunga che in taluni casi sono loro concessi specifici rimedi contrattuali[31]. Come meglio si specificherà nel prosieguo, la *reasonable expectation of privacy* viene in rilievo sia nell'ambito del lavoro pubblico sia nell'ambito del lavoro privato[32].

La frammentazione e la lacunosità della normativa sono evidentemente espressione di un sistema dove il mercato del lavoro è lasciato libero di agire, secondo il principio per cui le parti dovrebbero poter contrattare a loro piacimento[33].

2.1 Il contesto di lavoro pubblico

La sentenza capostipite in materia di sorveglianza del lavoratore nel settore pubblico è quella emanata dalla Corte Suprema nel caso *O'Connor v. Ortega* del 1987[34]. Infatti, pur non essendo il primo caso affrontato dai giudici di Washington, esso ha influenzato la giurisprudenza successiva in modo significativo.

Magno Ortega era un medico presso il Napa State Hospital incaricato prevalentemente di istruire le nuove leve. Nel 1981 il direttore generale dell'ospedale, Dennis O'Connor, si insospettì per alcuni acquisti fatti da Ortega, in particolare per un personal computer che

[26] D.J. SOLOVE, P.M. SCHWARTZ, *Privacy, Information, and Technology*, cit., 987-988. Vengono principalmente in rilievo l'*Electronic Communications Privacy Act* (18 U.S.C. § 2510 (2000)) e lo *Stored Communication Act* (18 U.S.C. §§ 2701-11 (2003), che non è altro che una parte del primo.

[27] S. DILUZIO, *Workplace E-mail: It's Not As Private As You Might Think*, 25 *Delaware Journal Of Corporate Law* 741 (2000), 755. Per una trattazione complete delle questioni legate alla privacy in ambito lavorativo nel sistema statunitense v. M.W. FINKIN, *Privacy in Employment Law*, Arlington, 2018.

[28] S. DILUZIO, *Workplace E-mail: It's Not As Private As You Might Think*, cit., 744. Un'eccezione è costituita dalla California che ha esteso mediante giurisprudenza la protezione accordata dalla costituzione ai dipendenti pubblici anche ai dipendenti privati (cf. *Porten v. University of San Francisco*, 134 Cal. Rptr. 839 (Cal. Ct. App. 1976), 842).

[29] Si veda S. DILUZIO, *Workplace E-mail: It's Not As Private As You Might Think*, cit., 745 ss., per una panoramica dell'applicabilità dell'*Electronic Communications Privacy Act* ai casi di violazione di privacy per le *e-mail* dei dipendenti. V. inoltre A.R. LEVINSON, *Workplace Privacy and Monitoring: The Quest for Balanced Interest*, 59 Cleveland State Law Review (2011), 4 ss., disponibile all'url: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893706..

[30] L. DETERMANN, R. SPRAGUE, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, cit., 990-993.

[31] D.J. SOLOVE, P.M. SCHWARTZ, *Privacy, Information, and Technology*, cit., 1094.

[32] A.R. LEVINSON, *Workplace Privacy and Monitoring: The Quest for Balanced Interest*, cit., 16. Cf. Restatement (Second) of Torts, § 652B.

[33] J.D.R. CRAIG, *Privacy and Employment Law*, cit., 58.

[34] 480 U.S. 409 (1987).

forse era stato acquistato con denaro proveniente dai pazienti su richiesta di Ortega. Il direttore generale era inoltre preoccupato da alcune accuse di molestie sessuali effettuate da colleghe a carico di Ortega e di maltrattamenti a danno di un paziente.
Ortega fu messo in aspettativa e il suo ufficio fu perquisito. Il medico agì in giudizio contro tale perquisizione e il caso raggiunse la Corte Suprema: tutti i giudici ritennero che il medico avesse una ragionevole aspettativa di privacy sulla sua scrivania e sul suo schedario. In particolare, l'opinione di maggioranza ritenne che l'aspettativa fosse riconducibile al fatto che a) il medico non condivideva né la sua scrivania né il suo schedario con altri colleghi; b) aveva occupato quell'ufficio per 17 anni e vi teneva oggetti personali; c) teneva i file relativi al lavoro fuori dall'ufficio; d) gli oggetti trovati nella perquisizione erano unicamente personali; e) l'ospedale non aveva apparentemente adottato alcun regolamento o *policy* interna che scoraggiasse i dipendenti dal conservare documenti ed effetti personali nelle loro scrivanie o schedari. Mentre tutti i giudici ritennero che Ortega avesse una aspettativa di privacy su scrivania e schedario, solo la maggioranza (5 su 9) considerò ragionevole l'aspettativa riguardo l'intero ufficio[35].
Ai fini del presente contributo vale la pena soffermarsi soltanto sulle modalità di determinazione della ragionevole aspettativa di privacy. Si può notare che due sono le categorie di indicatori presi in considerazione dalla Corte Suprema: da una parte, indici che si rifanno all'uso che l'interessato fa del luogo oggetto della perquisizione[36] e dall'altra parte, indici che si ricollegano alla sua conoscenza (o conoscibilità) di prassi applicate dal datore di lavoro. Si tratta di indici che permettono di effettuare una valutazione sull'aspettativa di privacy all'interno del singolo contesto e del singolo rapporto lavorativo, valutazione da farsi caso per caso[37]. Seguendo questi ragionamenti la Corte si spinse ad affermare che un ufficio pubblico può essere caratterizzato da un'apertura tale da non potersi avere alcuna aspettativa di privacy[38], situazione non verificatasi tuttavia nel caso di specie.
Nel più recente *United States v. Simons*[39], un dipendente del Foreign Bureau of Information Services (FBIS), una divisione della CIA, citò in giudizio l'amministrazione datrice di lavoro per un'ispezione sul suo computer che egli riteneva fosse stata effettuata in violazione del Quarto Emendamento. Durante una manutenzione effettuata in remoto, infatti, erano state scoperte sul computer di lavoro di Simons più di mille immagini pornografiche, alcune relative a minorenni. Fu creata una copia dell'hard disk da remoto e, successivamente, tale copia fu utilizzata per sostituire fisicamente il disco originale del computer di Simons. La sostituzione avvenne a opera di un collega, che consegnò

35 Il ragionamento si spostò poi sulla ragionevolezza che deve caratterizzare anche l'ispezione in sé. Nel caso di specie la maggioranza ritenne che la corte d'appello avesse errato nel valutare la ragionevolezza dell'ispezione e quindi la Corte Suprema ribaltò la decisione e la rinviò alla corte d'appello che riconobbe un risarcimento di oltre 600mila dollari, perché la ricerca aveva riguardato solo oggetti strettamente personali, era stata troppo ampia, e non era supportata dal sospetto che le informazioni si trovassero dove furono cercate; cf. *Ortega v. O'Connor*, 146 F.3d 119 (9th Cir. 1998).
36 In linea con *Oliver v. United States*, 466 U.S. 170 (1984), 178 (in tema di ispezioni e "open field doctrine").
37 *O'Connor v. Ortega*, cit., 717-718.
38 *O'Connor v. Ortega*, cit., 718. *Contra*: Justice Scalia nella sua opinione concorrente (*O'Connor v. Ortega*, cit., 729; 737).
39 *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000). Si veda anche *United States v. Monroe*, 50 M.J. 550 (A.F.C.M.R. 1999).

l'originale all'FBIS. Simons fu successivamente imputato per detenzione di materiale pedopornografico. Ritenendo che l'ispezione avesse violato i suoi diritti protetti dal Quarto Emendamento, il lavoratore richiese la soppressione delle prove ottenute mediante tale ispezione.

In questo caso la Corte d'appello del Quarto Circuito ritenne determinanti le *policy* interne al FBIS. Nel giugno del 1998, l'FBIS aveva adottato delle *policy* relative all'uso di Internet da parte dei dipendenti, che potevano accedere al web solo per affari governativi ufficiali. L'accesso a materiale illecito era proibito e le *policy* informavano i dipendenti che sarebbero stati effettuati controlli da remoto per assicurare l'adempimento a queste regole. Il materiale soggetto ad accertamento poteva includere, tra gli altri: file inviati e ricevuti, messaggi di posta elettronica in arrivo e in uscita, pagine web visitate[40]. Sulla base di queste *policy* nel luglio del 1998 furono effettuati i primi controlli da cui appunto emersero i materiali pornografici detenuti da Simons.

Alla luce del contenuto delle *policy* interne appena ricordato, la Corte ritenne che non vi fosse aspettativa di privacy o, per meglio dire, essa non poteva considerarsi ragionevole[41]. Pertanto il Quarto Emendamento non era stato violato dall'atto di copia dell'*hard disk*, e a maggior ragione non v'era stata violazione nella ricerca da remoto[42].

Parzialmente diverso il ragionamento per quanto concerneva l'ufficio: Simons aveva un ufficio personale, che non condivideva; non vi erano *policy* o usi interni che potessero avere l'effetto di diminuire l'aspettativa di Simons, che doveva pertanto considerarsi legittima[43]. Tuttavia non v'era violazione del Quarto Emendamento in quanto l'FBIS, pur in assenza di mandato, aveva uno "special need for the efficient and proper operation of the workplace"[44].

Nel caso *Leventhal v. Knapek* un dipendente del Dipartimento dei Trasporti lamentava che le ispezioni avvenute sul suo computer fossero state effettuate in violazione del Quarto Emendamento[45].

Considerate le circostanze, la corte ritenne che Leventhal avesse in effetti una ragionevole aspettativa di privacy: egli aveva uso esclusivo delle attrezzature presenti nell'ufficio, che non condivideva con nessuno. L'ufficio non era aperto al pubblico[46], né il Dipartimento dei Trasporti effettuava di norma ispezioni dei computer o aveva avvisato i dipendenti di non aspettarsi privacy nel contenuto dei computer[47]. Sebbene talvolta gli addetti al supporto tecnico accedessero ai computer del Dipartimento, le operazioni di manutenzione erano regolarmente annunciate. La loro scarsa frequenza, la loro selettività e il loro scopo contenuto non decretavano, secondo la Corte, il venir meno dell'aspettativa di privacy di Leventhal[48]. Pur sussistendo la aspettativa di privacy, considerato l'interesse

[40] *United States v. Simons*, cit., 395-396.
[41] In linea con il precedente *American Postal Workers Union v. United States Postal Serv.*, 871 F.2d 556 (6th Cir. 1989), 560.
[42] *United States v. Simons*, cit., 398-399; 401. Ancora una volta si fa riferimento a *O'connor et al. v. Ortega*, cit.
[43] *United States v. Simons*, cit., 399-400, citando i precedenti *O'Connor v. Ortega*, cit., 716-718 e 737; *Shields v. Burge*, 874 F.2d 1201 (7th Cir. 1989), 1203-04.
[44] *United States v. Simons*, cit., 400.
[45] *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001).
[46] Indice che potrebbe influire, come visto, sull'aspettativa di privacy: *O'Connor v. Ortega*, cit., 718.
[47] *Leventhal v. Knapek*, cit., 74, citando *United States v. Simons*, cit., 398.
[48] *Leventhal v. Knapek*, cit., 74.

pubblico all'ispezione, che era indirizzata a comprendere se vi fossero delle condotte sconvenienti da parte del dipendente, tra cui l'utilizzo di *software* non autorizzati, l'ispezione fu considerata lecita e non eccessivamente intrusiva rispetto alla natura della condotta del dipendente[49].

Nei due casi appena riassunti, la differenza fondamentale sta nell'aspettativa di privacy del dipendente: mentre nel caso di Leventhal le *policy* aziendali non avevano dato adito al lavoratore di sospettare ispezioni e monitoraggi, nel caso di Simons egli era stato preavvertito di tali possibilità. Nel primo caso l'aspettativa di privacy nasce legittimamente, mentre nel secondo no.

Una fattispecie particolare è quella al centro della sentenza della Corte d'Appello del Secondo Circuito nel caso *Sheppard v. Beerman*[50]: Sheppard era stato il *law clerk* di Beerman per alcuni anni, fino al suo licenziamento, avvenuto nel 1990 dopo che fra *clerk* e giudice v'era stato un litigio. Sheppard era stato intimato di andarsene senza poter prendere i propri effetti personali. Gli effetti personali del *clerk*, inclusi schedari, cassetti della scrivania, furono ispezionati da Beerman e da altri collaboratori; le schede che Sheppard aveva redatto personalmente riguardo ai casi decisi da Beerman furono rimosse dal suo ufficio e portate nell'ufficio del giudice per essere esaminate. Solo diversi giorni dopo questi eventi Sheppard poté tornare nel suo ufficio e recuperare i suoi oggetti e decise di agire in giudizio per violazione dei suoi diritti derivanti dal Quarto Emendamento da parte di Beerman[51].

La Corte ritenne che Sheppard non potesse nutrire una ragionevole aspettativa di privacy in quanto la relazione lavorativa fra giudice e *clerk* è unica nel suo genere: diversamente da una tipica relazione fra datore e dipendente, affinché la funzione giudiziaria sia efficiente è necessario che vi sia uno scambio libero di informazioni fra *clerk* e giudice. Questo implica che i *clerk* abbiano accesso a tutti i documenti relativi ai casi, nonché alle annotazioni personali del giudice, che a sua volta ha accesso ai documenti tenuti dal suo assistente. L'unicità di questa relazione lavorativa fa venire meno l'aspettativa di privacy in tutto ciò che pertiene l'ufficio del giudice, inclusi scrivanie, documenti e altre aree di lavoro[52].

Il caso *City of Ontario v. Quon* riguardava l'utilizzo da parte di un poliziotto di un cercapersone di cui era stato dotato dal dipartimento della polizia e che funzionava mediante rete *wireless*[53]. Le *policy* del dipartimento non ammettevano l'utilizzo di questa rete per benefici personali e il dipartimento si riservava il diritto di monitorare le attività della rete, specificando che gli utenti non avrebbero dovuto aspettarsi riservatezza. Non si specificava nulla riguardo ai messaggi, ma si chiariva che i messaggi sarebbero stati trattati come *e-mail*[54]. Uno dei dipendenti, Quon, sforò più volte il limite massimo di messaggi inviabili, finché il dipartimento richiese e ottenne dalla società gestrice della rete le trascrizioni dei contenuti di tali messaggi, che si rivelarono contenenti messaggi personali

[49] *Leventhal v. Knapek*, cit., 75, facendo riferimento a *O'connor et al. v. Ortega*, cit.
[50] *Sheppard v. Beerman*, 18 F.3d 147 (2d Cir. 1994).
[51] *Sheppard v. Beerman*, cit., 149-150.
[52] *Sheppard v. Beerman*, cit., 152.
[53] *City of Ontario v. Quon*, 560 U.S. 746 (2010).
[54] *City of Ontario v. Quon*, cit., 751.

e a sfondo sessuale. Il dipendente citò sia il dipartimento sia la società gestrice della rete, sostenendo di aver subito una violazione del Quarto Emendamento[55]. La Corte d'appello si interrogò circa l'esistenza di una protezione da parte di tale emendamento sui messaggi scambiati dagli ufficiali[56]. Essa ritenne che si dovevano considerare tali messaggi allo stesso modo di lettere o *e-mail*, e che, nonostante le *policy* ufficiali concedessero la facoltà di controllare la rete, informalmente questo non era mai avvenuto. Ciò dava adito a una aspettativa di privacy nei messaggi.
Il caso fu poi analizzato dalla Corte Suprema[57], che rovesciò la decisione della corte inferiore: per quanto il dipendente assumesse l'esistenza di un livello di privacy nei suoi messaggi, non era ragionevole per lui concludere che gli stessi messaggi fossero immuni da qualunque analisi. Come dipendente di un dipartimento di polizia avrebbe ragionevolmente dovuto sapere che poteva esserci la necessità di controllare i messaggi per comprendere se i cercapersone fossero utilizzati in maniera inappropriata. Considerando poi che l'ispezione dei messaggi era stata effettuata per legittimi scopi collegati al lavoro e non era stata eccessiva, essa doveva considerarsi ragionevole[58].
Riassumendo, dunque, con riferimento all'aspettativa di privacy dei dipendenti del settore pubblico un ruolo fondamentale hanno le *policy* aziendali[59]. Quando queste esplicitino la possibilità di effettuare perquisizioni ed ispezioni e siano conosciute dal dipendente, di fatto ne azzerano l'aspettativa di privacy. Non vale però il contrario: quando non vi siano *policy* interne, ciò non implica necessariamente che vi possa essere una ragionevole aspettativa di riservatezza[60]. Invero, giocano un ruolo fondamentale anche le consuetudini, di fatto "*policy* non scritte" di cui i lavoratori sono a conoscenza e che al pari delle *policy* riducono parzialmente o totalmente l'aspettativa perché si ritiene che il dipendente conosca e in qualche modo consenta – seppure implicitamente – l'intrusione nella sua sfera riservata[61]. La "realtà operativa" nella quale è immerso il dipendente può dunque avere effetti non trascurabili sulla sua aspettativa di riservatezza, incidendovi a vario titolo e spesso finendo per diminuirla o azzerarla[62].

2.2 Il contesto di lavoro privato

Il quadro del settore lavorativo privato non si differenzia in realtà molto da quello pubblico.

---

[55] I ricorrenti ritenevano violato anche lo *Stored Communications Act*, 18 U.S.C. Capitolo 121, §§ 2701–2712.
[56] *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. Cal., 2008). La Corte ritenne in ogni caso violato lo *Stored Communications Act* da parte della società gestrice della rete. In primo grado, la District Court aveva ritenuto esistente un'aspettativa di privacy ma aveva valutato come ragionevole l'ispezione dei messaggi*: Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116 (CD Cal. 2006).
[57] *City of Ontario v. Quon*, cit.
[58] *City of Ontario v. Quon*, cit., 761-762.
[59] L. DETERMANN, R. SPRAGUE, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, *26 Berkeley Tech. L.J. 979* (2011), 992-993.
[60] *O'Connor v. Ortega*, cit., 719.
[61] Si dà per assunto il consenso del lavoratore: S. WALLACH, *The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy*, *International Journal of Comparative Labour Law and Industrial Relations*, 191.
[62] *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), 751, riferendosi ancora una volta a *O'Connor v. Ortega*, cit., 725.

Nel caso *Smyth v. Pillsbury Co.* deciso nel 1997[63], la *United States District Court for the Eastern District of Pennsylvania* ritenne che l'utilizzo delle *e-mail* del sistema aziendale non potesse generare una ragionevole aspettativa di privacy. Essendo nel contesto privato, la ricorrente chiese che la società datrice fosse considerata responsabile non già di una violazione del Quarto Emendamento, bensì secondo la figura del *tort of intrusion upon seclusion*, per la configurazione del quale è comunque necessaria una ragionevole aspettativa di privacy in capo alla persona apparentemente danneggiata[64]. La Corte ritenne che non si potesse configurare tale aspettativa in quanto la ricorrente aveva inviato *volontariamente* delle comunicazioni al suo supervisore utilizzando il sistema di posta elettronica aziendale. Sebbene non esplicitamente richiamata in sentenza, sembra possibile ritenere che la Corte applicò la c.d. "third-party doctrine", secondo la quale chi fornisca volontariamente informazioni a terzi non può poi vantare su tali informazioni alcuna aspettativa di privacy[65]. Per queste ragioni l'aspettativa doveva considerarsi inesistente sebbene vi fossero state rassicurazioni sulle intercettazioni. Nel caso di specie inoltre la violazione non sembrò alla Corte considerevole e altamente offensiva, requisiti necessari per la configurazione del *tort*[66].

Di qualche anno successivo è il caso *McLaren v. Microsoft Corporation*[67] nel quale un dipendente della nota società statunitense aveva convenuto in giudizio quest'ultima sostenendo che essa, accedendo alle sue *e-mail* conservate in una "cartella personale" del suo computer di lavoro e divulgandole a terzi, avesse violato la sua privacy. La cartella personale in questione era accessibile solo attraverso una *password* scelta dal dipendente: McLaren riteneva che la possibilità di avere una cartella personale protetta da *password* avesse ingenerato in lui l'aspettativa che le *e-mail* non avrebbero subito intrusioni e interferenze, in sostanza un'aspettativa di privacy[68]; il ricorrente qualificava l'azione della

[63] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996)

[64] M.C. MCALLISTER, *Cell Phone Searches by Employers*, *99 Nebraska Law Review 937* (2021), 940.

[65] V. tra le tante la sentenza della Corte Suprema *Smith v. Mariland*, 442 U.S. 735 (1979), spec. 743-744. Sul tema si v. ad esempio R.M. THOMPSON II, *The Fourth Amendment Third-Party Doctrine*, Congressional Research Service Report, 2014, reperibile all'url: https://sgp.fas.org/crs/misc/R43586.pdf; M.W. PRICE, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, *8 Journal of National Security Law and Policy 247* (2016).

[66] *Smyth v. Pillsbury Co.*, cit., 101 (enfasi aggiunta). In senso conforme: *Bourke v. Nissan Motor Corp., U.S.A.*, No. B068705 (Cal. Ct. App. July 26, 1993); *Restuccia v. Burk Tech., Inc.*, 1996 Mass. Super. LEXIS 367 (Mass. Super. Aug. 13, 1996); *McLaren v. Microsoft Corp.,* 1999 Tex. Ct. App. LEXIS 4103 (Tex. App. May 28, 1999). In senso contrario si espresse un'altra corte nei medesimi anni (*United States v. Maxwell*, 45 M.J. 406 (U.S. Ct. App. Armed Forces 1996)), sebbene al di fuori del contesto lavorativo. In quel caso i giudici ritennero che colui che trasmette una *e-mail* abbia un'aspettativa ragionevole che la sua privacy non sarà violata; chiaramente questo scenario si modifica quando il messaggio giunge a destinazione, perché il mittente non ha più controllo su quanto accade alla *e-mail*. Una volta che una *e-mail* è spedita, fintanto che non venga "scaricata" dal destinatario, giace nei *server*. Fino ad allora il mittente ha un'aspettativa ragionevole legittima sulla riservatezza del messaggio spedito e il fatto che un *hacker* possa intercettare tale messaggio, non diminuisce l'aspettativa menzionata. Su questo ragionamento si basa anche la decisione: *Garrity v. John Hancock Mutual Life Insurance Co.*, 602002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002). V. anche M.A. POIRIER, *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?*, 60 U. Toronto Fac. L. Rev. 85 (2002), 90 ss. Per un commento alle prime decisioni inerenti il controllo della posta elettronica dei dipendenti v. P.F. GERHART, *Employee Privacy Rights In The United States*, 17 Comp. Lab. L.J. 175 (1995), spec. 199 ss.; P.E. HASH, C.M. IBRAHIM, *E-mail, Electronic Monitoring, And Employee Privacy*, 37 S. Tex. L. Rev. 893 (1996).

[67] *McLaren v. Microsoft Corporation*, cit.

[68] *McLaren v. Microsoft Corporation*, cit., 1-3.

società datrice come *tort of intrusion upon seclusion* secondo le leggi texane[69]. Microsoft, che secondo quanto emerso nel procedimento aveva "decriptato"[70] la password di accesso alla cartella di McLaren, sottolineava che nessuna norma del Texas riconosceva la privacy nel contenuto dei sistemi di posta elettronica forniti dal datore al dipendente nel contesto lavorativo. Si trattava, ancora una volta, di determinare l'aspettativa di privacy del lavoratore. A supporto della propria posizione il lavoratore si rifaceva a precedenti in cui si era riscontrata la presenza di aspettativa di privacy relativamente ad armadietti, forniti dal datore e chiusi con un lucchetto di proprietà del dipendente[71]: McLaren sosteneva che la sua cartella personale fosse analoga a un armadietto e che vi fosse solo una differenza nella tecnologia[72]. La Corte ritenne che l'argomentazione del ricorrente non potesse essere accolta in quanto, mentre nel caso richiamato l'armadietto era fornito ai dipendenti per riporvi effetti personali, il computer, l'*e-mail* e la cartella personale di McLaren gli erano stati forniti per scopi lavorativi e, dunque, erano meramente una parte intrinseca dell'ambiente lavorativo. In aggiunta, il meccanismo di funzionamento dell'*e-mail* richiede che ogni messaggio passi sulla rete e, dunque, sia a un certo punto accessibile da terzi (quantomeno dal *provider*) con ciò azzerando le aspettative di privacy del lavoratore[73]. In ogni caso, secondo la Corte texana, anche se vi fosse stata aspettativa di privacy, l'invasione di tale aspettativa da parte della società datrice non doveva considerarsi "altamente offensiva" per una persona ragionevole e, dunque, non si sarebbe qualificata come *tort of intrusion upon seclusion*[74].

Sempre con riferimento alle *e-mail*, il più recente caso *Walker v. Coffey*[75] conferma il *trend* fino a ora illustrato: il datore di lavoro può legittimamente acconsentire alle ispezioni dei luoghi o delle cose in uso ai dipendenti, in quanto esercita la sua "common-authority" su di essi[76]. Nel caso di specie, trattandosi di un indirizzo *e-mail* di lavoro, utilizzato all'interno del sistema di posta elettronica fornito dal datore, quest'ultimo esercitava la sua autorità su di esso e poteva dunque acconsentire all'ispezione[77]. La lavoratrice non poteva vantare aspettativa di privacy sia per tale ragione, sia per la applicazione, spesso ricorrente, della già citata "third-party doctrine"[78].

Non sono pochi i casi in cui la privacy del lavoratore concerne computer *files* o *e-mail*, come già visto peraltro per il contesto pubblico. I diversi fattori che le corti valutano per comprendere se vi sia o meno aspettativa in tali casi, sono stati riassunti come segue[79]: 1. L'azienda ha una politica che vieta l'uso personale o altri usi discutibili? 2. L'azienda

[69] Più precisamente come "intrusion upon the plaintiff's seclusion or solitude or into his private affairs", cfr. *McLaren v. Microsoft Corporation*, cit., 8.
[70] Questo il termine utilizzato nella sentenza: *McLaren v. Microsoft Corporation*, cit., 3.
[71] Il riferimento era a *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 63 (Tex. App.-Houston [1st Dist.] 1984).
[72] *McLaren v. Microsoft Corporation*, cit., 10-11.
[73] *McLaren v. Microsoft Corporation*, cit., 11-12.
[74] *McLaren v. Microsoft Corporation*, cit., 13.
[75] 905 F.3d 138 (2018).
[76] *Walker v. Coffey*, cit., 148-149. La *doctrine* della "common-authority" permette che un terzo acconsenta alle perquisizioni ed ispezioni sulla proprietà di un altro individuo in assenza di mandato, v. *United States v. Matlock*, 415 U.S. 164 (1974).
[77] *Walker v. Coffey*, cit., 149-150.
[78] *Walker v. Coffey*, cit., 146.
[79] *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005), 257.

controlla l'uso del computer o della posta elettronica del dipendente? 3. I terzi hanno il diritto di accedere al computer o alla posta elettronica? 4. L'azienda ha informato il dipendente, o il dipendente era a conoscenza, delle politiche di utilizzo e monitoraggio?[80]
Di fatto questo significa comprendere, come già visto nel contesto dell'impiego pubblico, se l'azienda avesse una *policy*, se la *policy* fosse conosciuta dal lavoratore e se tale *policy* fosse in essere ed effettivamente implementata al momento dei fatti[81]. Se a queste domande viene data risposta positiva, l'aspettativa di privacy del lavoratore non esiste o, comunque, non può essere ritenuta ragionevole.
Sempre con riferimento all'utilizzo di computer e Internet, vale la pena di illustrare un caso per molti versi simile a *United States v. Simons*, ma realizzatosi nel contesto del lavoro privato[82]. Jeffery Brian Ziegler era sospettato di detenere materiale pedopornografico, sospetto poi appurato da dei monitoraggi sul traffico Internet effettuato dal suo computer, a seguito dei quali due suoi colleghi fecero nottetempo due copie del disco rigido del computer. La compagnia datrice di lavoro consegnò all'FBI una copia dell'*hard disk* e il computer di Ziegler e gli esperti della scientifica appurarono effettivamente l'esistenza di immagini pedopornografiche. L'imputato richiedeva l'espulsione delle prove ottenute nell'ispezione effettuata dai suoi colleghi, perché in violazione del Quarto Emendamento, in quanto i colleghi di Ziegler avevano effettuato la copia su indicazione di un agente dell'FBI. Facendo riferimento al *leading case* Mancusi[83], la Corte ritenne che Ziegler avesse un'aspettativa di privacy riguardo al suo ufficio, che tra il resto era tenuto chiuso a chiave. Quindi quanto effettuato dai suoi colleghi era indubbiamente da considerarsi quale ispezione, ma un'ispezione acconsentita dal datore di lavoro. Tale consenso poteva ritenersi validamente prestato in quanto concernente cose di proprietà su cui il datore aveva un controllo e al cui contenuto, peraltro, il datore aveva possibilità di accedere. Ancora una volta, i lavoratori erano stati informati della possibilità di monitoraggio da parte della società ed erano avvertiti che i computer, di proprietà della società, erano da utilizzarsi solo per scopi lavorativi. Tenendo conto di tutte le circostanze, Ziegler non poteva quindi ragionevolmente attendersi che il suo computer fosse esente da ispezioni e, in ogni caso, la società datrice aveva legittimamente acconsentito all'ispezione, per cui le prove ottenute mediante l'ispezione non dovevano essere soppresse[84].
L'assenso del datore di lavoro fu cruciale anche in un più recente caso che vedeva coinvolto un ricercatore del dipartimento di medicina della New York University; si trattava ancora una volta di stabilire l'esistenza di una ragionevole aspettativa di privacy su un computer, più precisamente un pc portatile[85]. Il signor Zhu aveva ottenuto un portatile comprato con i fondi del National Institutes of Health, che utilizzava sia per motivi

[80] Nel caso di specie la questione riguardava l'"attorney-client privilege" in un procedimento per bancarotta, cfr. *In re Asia Global Crossing, Ltd.*, cit.
[81] *Dombrowski v. Governor Mifflin Sch. Dist.*, 2012 U.S. Dist. LEXIS 90674 (E.D. Pa. 2012), 18.
[82] *United States v. Ziegler*, 474 F. 3d 1184 (9th Cir. 2007).
[83] *Mancusi v. DeForte*, 88 S. Ct. 2120 (1968) è un caso fondamentale relativo all'aspettativa di privacy dei lavoratori suo luogo di lavoro. La Corte Suprema ritenne che Mancusi, sindacalista, avesse una aspettativa di privacy legittima e quindi fosse tutelato dal Quarto Emendamento, sul contenuto di alcuni documenti che egli teneva in un ufficio condiviso con altri sindacalisti. La corte ritenne che il fatto che condividesse con altri l'ufficio non togliesse valore alla sua aspettativa di privacy.
[84] *United States v. Ziegler*, cit., 1189-1193.
[85] *United States v. Yudong Zhu*, 23 F. Supp. 3d 234 (2014).

personali che professionali. Dopo averlo configurato, aveva creato numerose password e criptato il disco rigido. A seguito di sospetti per corruzione e frode, Zhu fu convocato di superiori e dai legali della NYU e in quell'occasione consegnò il proprio laptop, ma senza fornire le necessarie password. Il computer fu successivamente ispezionato dall'FBI, su autorizzazione del capo dell'area legale della NYU.

Prima della sua assunzione, Zhu aveva firmato un documento, intitolato "Policy Statement on Privacy, Information Security, and Confidentiality", il quale specificava che l'NYU poteva ispezionare i computer di sua proprietà così come quelli di proprietà dei dipendenti, per assicurarsi che essi fossero usati nel rispetto delle *policy* interne[86].

La Corte ritenne che l'aspettativa di privacy di Zhu potesse considerarsi ragionevole: nessuno poteva accedere al suo computer, che egli teneva in un ufficio privato o a casa. L'utilizzo da parte del ricercatore di password e cifrature deponeva nello stesso senso[87]. Tuttavia, l'ispezione poteva considerarsi valida secondo la teoria del "third-party consent", perché firmando i documenti, il ricercatore aveva conferito legalità all'accesso da parte della NYU. Inoltre, erano presenti tutti i requisiti necessari perché si potesse trattare di un valido consenso da parte di terzi: il terzo esercitava un'autorità sul computer, aveva un interesse sostanziale nello stesso e aveva il permesso di accedervi. Per questi motivi l'ispezione da parte dell'FBI poteva considerarsi valida e non infrangeva il Quarto Emendamento[88].

Nel caso *Pike v. Hester*[89], quest'ultimo aveva effettuato un'ispezione dell'ufficio di Pike in assenza di mandato. Hester era un sergente presso l'ufficio dello sceriffo di Elko County. Pike era il direttore del settore ricreativo della stessa contea e lavorava in un ufficio condiviso con il proprio assistente presso il *Jackpot Recreation Center*. Per motivi non attinenti al lavoro[90], Pike e Hester non avevano un buon rapporto. Un giorno Hester, approfittando della macchina di servizio e delle sirene, fermò il capo di Pike (Lynn Forsberg) e gli disse che riteneva che alcuni dipendenti spacciassero droga all'uscita dell'edificio dove lavoravano. Chiese anche il permesso di poter effettuare un'ispezione negli uffici e non molto tempo dopo effettuò un'ispezione notturna all'interno del *Recreation center*. Insieme a Ester vi erano un altro poliziotto e un cane antidroga, che però non rinvenne alcuna traccia di stupefacenti. Quando Pike venne a sapere citò in giudizio Hester sostenendo che l'ispezione avesse violato il Quarto emendamento: il capo di Pike infatti non aveva dato il proprio consenso all'ispezione e Hester non aveva alcuna autorità per effettuare l'ispezione di sua spontanea volontà e in autonomia. La *District court* ritenne che si potesse applicare il Quarto Emendamento e che Pike avesse una ragionevole

86 *United States v. Yudong Zhu*, cit., 236. Zhu aveva firmato anche uno "Staff Handbook and the Code of Conduct Handbook" che chiariva che computers, *e-mail*, attrezzature e comunicazioni elettroniche erano di proprietà esclusiva della NYU e che lo staff non avrebbe dovuto avere alcuna aspettativa di privacy. Aggiungeva che le attrezzature, incluse quelle utilizzate a casa, potevano essere ispezionate ed esaminate in ogni momento (*United States v. Yudong Zhu*, cit., 237). Tale documento, tuttavia, non si applicava ai "members of the Faculty" dei quali lo stesso Zhu era parte (cfr. *United States v. Yudong Zhu*, cit., 240).

87 *United States v. Yudong Zhu*, cit., 238-239.

88 *United States v. Yudong Zhu*, cit., 240-242.

89 891 F.3d 1131 (2018).

90 Pike era allenatore di football in una scuola superiore per una squadra nella quale giocava anche uno dei figli di Hester. In tale veste Pike aveva ripreso più volte il figlio di Ester e talvolta lo aveva lasciato in panchina. Questo evidentemente non piaceva al padre del ragazzo; cf. *Pike v. Hester*, cit., 1134.

aspettativa di privacy sul suo ufficio, aspettativa che non veniva meno in quanto, sebbene dalle *policy* interne il capo di Pike potesse esprimere un valido consenso all'ispezione, non era stato appurato se tale consenso vi fosse o meno[91]. Il fatto che l'ispezione fosse stata effettuata mediante un cane antidroga non significava che l'aspettativa di privacy svanisse: tali ispezioni sono state ritenute valide quando effettuate in luoghi pubblici o l'obiettivo dell'ispezione era già lecitamente posseduto[92].

L'analisi che precede cerca di fornire un quadro sufficientemente esaustivo del sistema statunitense, inevitabilmente dispersivo. Tuttavia, si può notare come le decisioni siano quasi tutte dello stesso segno[93]: da più parti è stato sottolineato come sia difficile riscontrare sentenze di diversa soluzione rispetto a quelle qui elencate[94].

È stato fatto notare come in *Quon* la Corte Suprema abbia perso un'occasione per delimitare l'area della privacy che non può essere limitata o distrutta dall'esistenza di *policy*, ma tale occasione non è stata colta[95]. Il livello di dettaglio delle singole informative fornite ai dipendenti potrebbe giocare un ruolo decisivo, tuttavia le Corti statunitensi tendono in generale a interpretare le informative in senso ampiamente favorevole ai datori di lavoro, per cui anche *policy* poco chiare o semplicistiche sono ritenute sufficienti a supportare l'interesse del datore a tutelare il proprio *business*[96].

III. L'ESPERIENZA CANADESE

Il sistema canadese di protezione della privacy e dei dati personali si articola su più livelli normativi, fornendo una tutela completa per entrambi i diritti[97].

Lo scenario è stato modificato profondamente nel 2001, con l'intervento federale del *Personal Information Protection and Electronic Documents Act* (PIPEDA)[98]. La novità introdotta da questo testo è principalmente quella del suo ambito di applicazione: con il PIPEDA,

---

91 *Pike v. Hester*, cit., 1137; v. anche la *dissenting opinion*, 1142 ss.

92 *Pike v. Hester*, cit., 1140-1142.

93 S. DILUZIO, *Workplace E-mail: It's Not As Private As You Might Think*, cit., 754. Si veda nello stesso segno la più recente *Dombrowski v. Governor Mifflin School District*, cit.

94 V. sul punto D.C. DAMMEIR, *Fading Privacy Rights of Public Employees*, 6 Harvard Law & Policy Review 297 (2012), spec. 305 ss. Per un riassunto delle varie motivazioni alla base delle decisioni giurisprudenziali che negano la privacy del lavoratore v. M. ECHOLS, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using* Respondeat Superior *to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 Computer L. Rev. & Tech. J. 273 (2003), 285-286; 290 ss.

95 L. DETERMANN, R. SPRAGUE, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, cit., 1016. Al contrario, la Corte ha esplicitato di non voler assumere decisioni che potessero definire l'esistenza e l'ampiezza di aspettative di privacy dei lavoratori dipendenti, cfr. *City of Ontario v. Quon*, cit., 757.

96 L. DETERMANN, R. SPRAGUE, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, cit., 1017-1018.

97 Per quanto riguarda più in particolare la privacy dei lavoratori, si veda il contributo di J. DEBEER, *Employee Privacy: the Need for Comprehensive Protection*, 66 Saskatchewan Law Review 383 (2003).

98 Per un approfondimento sulla storia dell'adozione del PIPEDA, v. S. PERRIN, H.H. BLACK, D.H. FLAHERTY, T. MURRAY RANKIN, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Toronto, 2001, 1 ff. Il PIPEDA si basa sulle *Guidelines of the Organisation for Economic Co-operation and Development* (OECD), cf S. PERRIN, H.H. BLACK, D.H. FLAHERTY, *The Personal Information Protection and Electronic Documents Act*, cit., 22; W.A. CHARNETSKI, P.D. FLAHERTY, J. ROBINSON, *The Personal Information Protection and Electronic Documents Act. A Comprehensive Guide*, Aurora, 2001, 9.

infatti, la raccolta, l'uso e la diffusione di informazioni personali sono per la prima volta regolamentate anche nel settore privato[99].

L'*Act*, che verosimilmente sarà pesantemente rivisto nel prossimo futuro[100], prevede che ogni raccolta, utilizzo e diffusione di informazioni personali possa avvenire solo per scopi che una "reasonable person" considererebbe appropriati nel caso concreto[101]. Declinando questa previsione nel contesto lavorativo, ciò significa che il consenso del lavoratore è elemento necessario ma non più sufficiente a giustificare la sorveglianza delle attività lavorative[102]. In secondo luogo, la normativa in discorso obbliga ciascuna organizzazione a designare un soggetto responsabile della conformità dell'organizzazione alle normative sulla privacy[103]: ciò può essere visto quale forma di garanzia per il lavoratore, che non sottostà semplicemente e puramente alla sorveglianza del datore di lavoro, ma può contare sulla presenza di un soggetto a tutela della sua privacy[104]. Inoltre, le varie previsioni sul consenso alla raccolta dei dati, nonché sui limiti e le finalità di quest'ultima[105], arginano la discrezionalità del datore.

Nonostante la presenza del PIPEDA, la contemporanea vigenza di diversi testi legislativi a livello di ciascuna provincia canadese finisce per creare una certa disomogeneità rispetto alla protezione della privacy dei lavoratori: le normative statali continuano infatti a essere applicabili, pur in presenza di un'omnicomprensiva disciplina quale il PIPEDA, laddove le stesse siano "sostanzialmente simili" a quest'ultima.[106]

---

[99] In particolare la parte prima titolata: "Protection of personal information in the private sector". In precedenza, la regolamentazione della protezione dei dati personali nel settore privato era affidata a una normativa settoriale e frammentata, vale a dire riferita soltanto ad alcuni settori dell'economia (cf. B. MCISAAC, R. SHIELDS, K. KLEIN, *The law of privacy in Canada*, Toronto, 2007, 1-51).

[100] Al momento della stesura del presente articolo, pende il Bill C-27 "Digital Charter Implementation Act, 2022" che introdurrebbe tre normative: il Consumer Privacy Protection Act ("CPPA"), il Personal Information and Data Protection Tribunal Act ("PIDPTA") e l'Artificial Intelligence and Data Act ("AIDA"). Se questo disegno di legge fosse poi adottato, PIPEDA diverrebbe l'"Electronic Documents Act", perdendo la sua parte relativa alla privacy.

[101] PIPEDA, sez. 5(3). Si veda anche PRIVACY COMMISSIONER OF CANADA, *Annual Report to Parliament 2000-2001*, 19, reperibile all'url: http://www.priv.gc.ca/information/ar/02_04_09_e.pdf

[102] M. GEIST, *Computer and E-mail Workplace Surveillance In Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance*, 2002, 22, reperibile all'url: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_en.pdf (pubblicato anche in 82 Canadian Bar Review 151 (2003)).

[103] PIPEDA, Schedule 1, Principle 4.1 – Accountability.

[104] M. GEIST, *Computer and E-mail Workplace Surveillance In Canada*, cit., 23.

[105] Rispettivamente in PIPEDA, Schedule 1, Principi 4.3 (Consent), 4.4 (Limiting collection); 4.2 (Identifying purposes). Si devono però menzionare le specifiche eccezioni alla necessità di consenso preventivo previste alla sezione 7 del PIPEDA; fra queste è emblematica l'ipotesi della sezione 7(1)(b) secondo cui è lecita la raccolta di dati personali senza la conoscenza e il consenso dell'individuo quando questi comprometterebbero la disponibilità o l'accuratezza delle informazioni, la cui raccolta è ragionevolmente effettuata per scopi collegati, ad esempio, alla violazione di un contratto o di una legge canadese. Anche il divieto di diffusione dei dati subisce delle eccezioni: a titolo d'esempio, si consideri che il PIPEDA permette l'utilizzo di dati personali senza consenso se ciò possa essere utile in un'investigazione che riguardi la violazione di una legge canadese o straniera (cfr. sez. 7(2)(a)).

[106] Dal 1° gennaio 2004, il PIPEDA è applicabile a tutte le attività commerciali in ciascuna provincia canadese che non abbia introdotto una legislazione "sostanzialmente simile". Al tempo dell'emanazione del PIPEDA soltanto il Québec aveva già adottato una disciplina interna per la protezione dei dati personali (*Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1). Solo nel 2004 anche le province del British Columbia e dell'Alberta adottarono una regolamentazione interna in materia (rispettivamente *Personal Information Protection Act*, S.B.C. 2003, c. 63 e *Personal Information Protection Act,* S.A. 2003, c. P-6.5). Ritengono disomogenea la protezione dei lavoratori fra le diverse province J. DEBEER, *Employee Privacy: the Need for*

Si deve sottolineare, inoltre, che in conseguenza alla divisione costituzionale dei poteri fra federazione e stati, il PIPEDA si applica soltanto a settori lavorativi che siano regolamentati a livello federale[107]. Ciò significa che i lavoratori delle province in cui non vi sia una regolamentazione statale sulla privacy e che siano impiegati in settori regolati da normative provinciali, non godranno della protezione offerta dal PIPEDA.
Il PIPEDA si affianca al precedente *Privacy Act* del 1983[108], il cui ambito di applicazione è tuttavia ristretto alle istituzioni governative federali[109].
Devono essere menzionati anche gli interventi di alcune province canadesi che hanno introdotto con legge una specifica figura di *tort* per "invasion of privacy", che considera illecita l'invasione di privacy che sia irragionevole nelle circostanze, quando il danneggiante agisca con dolo[110]. Per quanto però riguarda il contesto lavorativo, esiste una specifica eccezione inerente il rapporto di lavoro: è un principio generalmente accettato nel diritto del lavoro canadese che quando un individuo entri in un nuovo rapporto di lavoro, acconsente implicitamente al modo in cui tale lavoro è gestito dal datore. Ciò vale anche per attività di monitoraggio e sorveglianza dei dipendenti[111].
A monte di questi interventi legislativi si pone poi la *Charter of Rights and Freedoms*. Ciò che è fondamentale chiarire fin da principio è che la Carta si applica esclusivamente alle azioni poste in essere dalla Corona, ovverosia dai vari livelli di governo e da altri attori statali. Pertanto, sebbene la Corte suprema abbia affermato a più riprese che le corti dovrebbero

Comprehensive Protection, cit., 407-408; A. LEVIN, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, 22 Canadian Journal of Law and Society 197 (2007), 199. Si veda quest'ultimo contributo per una disamina delle menzionate legislazioni provinciali in tema di privacy dei lavoratori.

107 A. LEVIN, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, cit., 200. Cf. PIPEDA, SEZ. 4(1)(b) – Application.

108 R.S.C. 1985, c. H-6.

109 In verità, la prima regolamentazione dei dati personali si ebbe nel 1977 con l'introduzione del *Canadian Human Rights Act*, che conteneva una previsione inerente la materia qui esaminata, ma che fu poi abrogata e sostituita mediante il *Privacy Act*. A differenza di quanto accade per il settore privato, in ambito pubblico tutte le provincie canadesi, eccetto il New Brunswick, hanno emanato una normativa statale. Fondamentale innovazione introdotta dal *Privacy Act* è il *Privacy Commissioner*, che, sebbene non abbia il potere di emettere decisioni vincolanti, può comunque fornire pareri e raccomandazioni sull'utilizzo dei dati personali. La sua attività è stata estesa con il PIPEDA anche all'ambito di applicazione di quest'ultimo. Cf. MCISAAC ET AL., *The law of privacy in Canada*, cit., 3-5.

110 Si tratta delle province del British Columbia, Manitoba, Newfoundland e Saskatchewan, che hanno emanato rispettivamente i seguenti interventi normativi: R.S.B.C. 1996, c. 373; R.S.M. 1987, c. P125; R.S.S 1978, c. P-24; S.N. 1981, c. 6, tutti denominati "Privacy Act". Il requisito del dolo è assente nella fattispecie prevista dal *Privacy Act* del Manitoba. Nelle altre province canadesi non esiste una figura di *tort* a difesa della privacy, in quanto non è mai stata riconosciuta nel *common law*. Solo molto di recente, la Corte d'Appello dell'Ontario in *Jones v. Tsige*, (2012 ONCA 32) ha esplicitamente riconosciuto un "right of action for intrusion upon seclusion". La nomenclatura rimanda immediatamente alla classificazione dei *privacy torts* statunitensi effettuata da W. PROSSER, *Privacy*, cit., 389 ss. Nella sentenza citata, la Corte dell'Ontario ha classificato l'intrusione in questioni lavorative come "highly offensive" (cf. *Jones v. Tsige*, cit., par. 72). La stessa sentenza cita una serie di contributi dottrinali a sostegno del riconoscimento di questo *tort* (cfr. *Jones v. Tsige*, cit., par. 66).

111 A. LEVIN, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, cit., 205. Per una panoramica della protezione della privacy del lavoratore precedente all'introduzione del PIPEDA v. J.D.R. CRAIG, *Privacy and Employment Law*, Toronto, 1999, 131 ss. Particolare importanza è data anche alle previsioni del Criminal Code che puniscono le intercettazioni di conversazioni private, v. ad esempio C. MORGAN, *Employer Monitoring of Employee Electronic Mail and Internet Use*, 44 McGill L. J. 849 (1999), 874 ss. V. lo stesso contributo (879 ss.) anche per una panoramica di altre normative pre-PIPEDA che tangenzialmente proteggevano il diritto alla privacy in specifici settori.

incorporare i valori della Carta nelle interpretazioni relative alla privacy nei rapporti fra privati, la Carta stessa risulta poco utile in tali contesti[112].

Nonostante nella *Charter* non vi sia una previsione specifica a tutela della privacy[113], essa è ricondotta alle sezioni 7 e 8[114]. Nei casi che qui ci interessano, la lesione della riservatezza e del diritto alla protezione dei dati personali è fatta risalire alla sezione 8, interpretandola alla luce delle sentenze della Corte Suprema statunitense sul Quarto emendamento, essendo le due previsioni legislative assai simili fra loro[115]. La Corte Suprema canadese ha peraltro ritenuto che la sezione 8 estenda la propria protezione anche alle informazioni personali[116]. Il parametro da considerare sarà la "reasonable expectation of privacy", da valutarsi, secondo quanto stabilito dalla *Supreme Court* nel caso *R. v. Plant*, sulla base dei seguenti elementi: l'informazione in sé, la natura della relazione fra la parte che rivela l'informazione e la parte che la considera confidenziale, il luogo dove l'informazione è stata ottenuta, il modo in cui fu ottenuta e, per le ipotesi di reato, la serietà del crimine sotto indagine[117].

Nel *case law* sono state riconosciute tre differenti "zone" di privacy: territoriale, quale quella che un soggetto dovrebbe godere nelle mura di casa propria; personale o corporea, quando riguardi il corpo umano o la personalità fisica; e informazionale, che protegge i dettagli intimi di una persona[118]. Ci sono inoltre due parametri secondo cui valutare il diritto alla privacy di un soggetto: 1) l'intensità con cui la libertà o la sicurezza di un individuo è minacciata dall'intrusione statale nei suoi affari personali; 2) l'estensione dell'aspettativa ragionevole di privacy dell'individuo[119]. Per quanto più in particolare riguarda quest'ultimo

---

112 S. PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 7. V. anche J. DEBEER, *Employee Privacy: the Need for Comprehensive Protection*, cit., 394. V. le decisioni della Corte suprema in *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573; *McKinney v. University of Guelph*, [1990] 3 S.C.R. 229; *Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130.

113 Nel 1987 la "Commissione giustizia" della *House of Commons* canadese suggerì di prendere in considerazione la creazione di un diritto costituzionale alla privacy, che tuttavia non fu mai introdotto. Si veda a tal proposito il contributo di D.H. FLAHERTY, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 Case W. Res. L. Rev. 831 (1991), che discute circa l'opportunità di tale eventuale modifica costituzionale.

114 Si veda sulla sez. 7 della Carta, R.J. SHARPE, K. ROACH, *The Charter of Rights and Freedoms*, cit., 219 ss; sulla sez. 8 v. IBIDEM, 272 ss.. La sezione 7 si riferisce al diritto alla vita, alla libertà e alla sicurezza della persona e al diritto di non essere privati di questi se non secondo i principi di giustizia. Secondo la giurisprudenza della Corte Suprema, alcune ipotesi di lesione della privacy possono essere ricondotte al diritto alla libertà e alla sicurezza della persona e pertanto ricomprese in questa sezione, v. ad es. *R. v. O'Connor*, [1995] 4 S.C.R. 411; *M. (A.) v. Ryan*, [1997] 1. S.C.R. 157.

115 Cf. la sentenza *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, par. 23. La Corte Suprema canadese fece riferimento al famoso caso statunitense *Katz v. United States*, cit., di interpretazione del Quarto Emendamento della Costituzione americana, con contenuto molto simile alla Sezione 8 della *Canadian Charter of Rights and Freedoms*.

In sostanza si applicherà la sezione 8 quando la privacy sia invasa da un "search or seizure", mentre si applicherà la sezione 7 come protezione costituzionale al di fuori di tali ipotesi secondo MCISAAC ET AL., *The law of privacy in Canada*, cit., 2-9.

116 *R. v. Plant*, [1993] 3 S.C.R. 281.

117 *R. v. Plant*, cit., par. 26.

118 In questi termini *Ruby v. Canada (Attorney General)*, [2000] 3 F.C. 589 (C.A.), par. 166. Si veda comunque già *R. v. Dyment*, [1988] 2 S.C.R. 417, par. 30.

119 Si veda ancora *Ruby v. Canada (Attorney General)*, cit., par. 168. L'aspettativa di privacy è protetta principalmente dalla sezione 8.

aspetto, l'esistenza e la profondità di una aspettativa di privacy devono essere decise caso per caso[120].

In questo contesto si inscrivono alcune importanti decisioni relative all'ambiente lavorativo[121].

Nel 1999 la Corte Suprema del British Columbia decise il caso *Pacific Northwest Herb Corp. v. Thompson*[122]. La fattispecie riguardava un dipendente della Pacific Northwest che utilizzava un computer della società anche per scopi personali. Dopo essere stato licenziato continuò tale utilizzo. Prima di restituire il computer alla società, Thompson chiese a una società specializzata che cancellasse tutti i dati contenuti sul disco fisso, sia quelli di lavoro, che quelli personali. Ciò nonostante, quando il datore di lavoro rientrò in possesso del computer, riuscì a recuperare i dati, fra cui vi erano anche delle informazioni circa un'azione di impugnazione del licenziamento che Thompson pensava di esperire nei confronti della Pacific Northwest. L'*ex* dipendente sostenne di avere un diritto alla privacy nei dati trovati sul disco fisso. Il giudice ritenne che in effetti Thompson avesse una ragionevole aspettativa di privacy in relazione a quei documenti che erano stati creati per utilizzo famigliare o personale[123].

Nel caso *Briar v. Canada (Treasury Board)* del 2003[124], alcuni dipendenti di un carcere di massima sicurezza contestarono le sanzioni loro comminate dal datore di lavoro per lo scorretto utilizzo delle *e-mail* della società. Pur essendo stati più volte avvertiti delle *policy* aziendali in fatto di uso inappropriato della posta elettronica, alcuni funzionari utilizzarono l'*e-mail* per scambiarsi foto a contenuto pornografico. Il datore scrisse a tutti i dipendenti specificando che tali tipi di contenuti dovevano considerarsi inaccettabili e quindi dovevano essere rimossi. Successivamente a 54 dipendenti furono comminate sanzioni di vario genere e quattro di loro impugnarono la sanzione, lamentando una violazione della sezione 8 della *Charter*. Tuttavia non furono in grado di dimostrare una ragionevole aspettativa di privacy: secondo il giudicante, infatti, non solo non v'era stato un monitoraggio, o una ispezione sulle persone o sulle cose, ma i funzionari avrebbero dovuto rendersi conto che una volta spedita un'*e-mail*, si perde il controllo sulla stessa. A ciò doveva aggiungersi il contenuto moralmente ripugnante delle *e-mail*, per il quale i dipendenti non potevano attendersi legittimamente della privacy[125].

---

120 Nel caso *R. v. Edwards*, [1996] 1 S.C.R 128, par. 45, la Corte Suprema elencò una serie di fattori da prendere in considerazione per determinare l'aspettativa di privacy. Si veda, per un'applicazione *R. v. Tessling*, [2004] 3 S.C.R. 432, par. 32 ss, che applica un test cosiddetto della "totalità delle circostanze".

121 Per una breve disamina dei risvolti giuridici del controllo delle *e-mail* da parte del datore di lavoro prima dell'introduzione del PIPEDA, v. H.L. RASKY, *Can an employer search the contents of its employees' e-mail?*, 20 Advocacy Quarterly 221 (1998).

122 *Pacific Northwest Herb Corp. v. Thompson*, [1999] B.C.J. No. 2772. Il caso vedeva applicarsi il *Privacy Act* della provincia del British Columbia.

123 *Pacific Northwest Herb Corp. v. Thompson*, cit., par. 26. La decisione fu di questo segno nonostante la proprietà del computer fosse pacificamente riconosciuta del datore di lavoro. La questione inerente alla proprietà del computer contenente informazioni personali è sollevata anche della sentenza in commento. V. *infra*.

124 *Briar v. Canada (Treasury Board)*, 116 L.A.C. (4th) 418 (2003).

125 *Briar v. Canada (Treasury Board)*, cit., par. 59-60. In questa sentenza si fece riferimento al caso statunitense *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (U.S. Dist. Ct. E.D. Penn. 1996), in cui la corte statuì che non v'è *reasonable expectation of privacy* in comunicazioni effettuate tramite il sistema di posta elettronica aziendale, nemmeno se un datore di lavoro assicuri ai suoi dipendenti che le *e-mail* non saranno intercettate. Nello stesso senso, più di recente: *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004).

Altro caso simile, citato anche in *Briar v. Canada*, fu deciso nel 1999 in sede arbitrale[126]: un dipendente era stato licenziato per aver scritto un'*e-mail* fortemente critica nei confronti del datore di lavoro e dei colleghi a un sito *web* di un sindacato, utilizzando il sistema di posta elettronica aziendale. Secondo l'arbitro qualunque utente informato che utilizzi la posta elettronica sa che i messaggi possono essere monitorati e che comunque non si ha controllo sulle *e-mail* una volta messe in circolazione[127]. Questi due elementi convinsero l'arbitro che non vi poteva essere una legittima aspettativa di privacy[128].
In un altro caso, l'arbitro ritenne che quando non vi è una *policy* specifica, un dipendente non può avere una legittima aspettativa di privacy rispetto a *e-mail* ricevute e spedite sul posto lavoro, attraverso gli strumenti datoriali nell'orario lavorativo[129]. Del medesimo segno la sentenza della Corte d'Appello dell'Alberta che sancì esplicitamente che sulle informazioni contenute all'interno di un computer di lavoro non si può generare un'aspettativa di privacy. La Corte sottolineò come il luogo di lavoro non sia l'abitazione del lavoratore e che, anche qualora il datore permetta un limitato uso dei computer di lavoro, egli potrà determinare condizioni e termini di tale utilizzo[130].
Quanto detto fa in realtà riferimento solo a ipotesi in cui non esista uno "statutory privacy right": invero, sebbene le informazioni lavorative non siano di norma considerate "personali", informazioni intime che siano comunque correlate al lavoro rimangono invece "personali"[131].
Per molto tempo furono pochissime le decisioni di senso opposto a quelle finora riassunte. Fra queste, una decisione arbitrale che ritenne che il diritto del datore di ispezionare i contenuti del computer di un dipendente dovesse essere bilanciato con l'aspettativa di privacy del lavoratore e fosse soggetto a un test di ragionevolezza[132]. In sostanza la prevalente giurisprudenza canadese in tema di privacy del lavoratore sulle informazioni contenute nel sistema aziendale sosteneva l'inesistenza di una legittima aspettativa di privacy[133].

---

[126] *Camosun College v. C.U.P.E., Local 2081*, [1999] B.C.C.A.A.A. No. 490. I lavoratori facenti parte di un sindacato vedono normalmente riconosciuto un diritto alla privacy da parte delle decisioni arbitrali che in genere decidono sui contratti collettivi. Le decisioni arbitrali in questa materia sono molte, in quanto i contratti collettivi canadesi debbono includere una clausola che prevede la decisione in sede arbitrale delle controversie scaturenti dei contratti medesimi, v. J.D.R. CRAIG, *Privacy and Employment Law*, cit., 125.
[127] V. su quest'ultimo elemento anche un'altra decisione arbitrale: *Naylor Publications Co. (Canada) and Media Union of Manitoba, Local 191 (Re)*, [2003] M.G.A.D. No. 21.
[128] *Camosun College v. C.U.P.E., Local 2081*, cit., par. 21.
[129] *Milsom v. Corporate Computers Inc.*, [2003] A.J. No. 516 (Atla. Q.B.), par. 41.
[130] *Poliquin v. Devon Canada Corporation,* 2009 ABCA 216.
[131] D. MICHALUK, *Employer Access to Employee E-mails in Canada*, 6 Canadian Privacy Law Review 94 (2009), 96. V. anche *University of British Columbia (Re)*, 2007 CanLII 42407 (BC I.P.C.); *Johnson v. Bell Canada*, [2008] F.C.J. No. 1368.
[132] *Lethbridge College and Lethbridge College Faculty Assn. (Bird Grievance) (Re)*, [2007] A.G.A.A. No. 67, par. 31.
[133] D. MICHALUK, *Employer Access to Employee E-mails in Canada*, cit., 95 e casi ivi citati alla n. 18. Decisioni in senso contrario si possono vedere in alcune decisioni arbitrali, quali *Lethbridge College and Lethbridge College Faculty Assn. (Bird Grievance) (Re)*, [2007] A.G.A.A. No. 67, in cui fu ritenuto che il diritto del datore di ispezionare i contenuti del computer di un dipendente deve essere bilanciato con l'aspettativa di privacy del lavoratore ed è soggetto ad un test di ragionevolezza, v. *Ibidem*, par. 31. Più in generale, il diritto alla privacy necessita di essere sempre bilanciato con gli altri diritti che entrano in gioco, nel contesto specifico; cf. *R. v. Duarte*, [1990] 1 S.C.R. 30, 45.

Lo scenario ha subito un cambiamento drastico con una importante decisione della Corte Suprema: *R. v. Cole*, datata 2012[134]. Cole era un insegnante di scuola superiore a cui era stato affidato un computer per ragioni lavorative, ma che lo stesso poteva utilizzare anche per motivi personali. Durante un'ordinaria manutenzione, un tecnico aveva scoperto una cartella nascosta contenente fotografie di una studentessa minorenne parzialmente nuda. Il tecnico lo comunicò al preside e fece copia delle fotografie su un compact disc. Il preside sequestrò il computer e i tecnici della scuola copiarono i file temporanei di Internet su un secondo compact disc. Il computer ed entrambi i dischi furono portati alla polizia, che senza mandato ne esaminò il contenuto e creò una "copia esatta" dell'hard disk per scopi investigativi. Cole chiese la soppressione delle prove perché raccolte in violazione della Section 8, secondo quanto disposto dalla Section 24(2) della stessa Carta[135].

Al fine di valutare se Cole potesse o meno vantare una ragionevole aspettativa di privacy la Corte canadese si rifece al suo famoso precedente *R. v. Morelli*[136], un caso per molti aspetti analogo a *R. v. Cole*, con la differenza che il materiale pedopornografico era stato rinvenuto sul computer personale di Morelli e non su quello di lavoro. Anche in quel caso l'imputato chiedeva che le prove fossero espunte perché ottenute violando la sezione 8. La Corte aveva ritenuto che l'ispezione di un computer in violazione della sezione 8 avesse un forte impatto sulla privacy, in considerazione del contenuto spesso molto personale conservato sui personal computer[137].

La Corte suprema sottolineò che nel contesto canadese la privacy è una questione di aspettative ragionevoli: la sua protezione da parte della *Charter* dipende appunto dalla ragionevolezza dell'aspettativa, cioè se persone informate, trovandosi nella stessa posizione dell'accusato, si aspetterebbero di avere della privacy[138].

Per comprendere se Cole avesse o meno un'aspettativa di privacy la Supreme Court of Canada applicò il c.d "totality of the circumnstances test", elaborato nel precedente *R. v. Edwards*[139]. Il test è composto da quattro punti: (1) valutare il materiale esaminato dall'ispezione; (2) valutare la possibilità di un interesse diretto nel materiale da parte del ricorrente; (3) indagare circa l'eventuale aspettativa soggettiva di privacy dello stesso ricorrente; (4) giudicare se l'aspettativa fosse oggettivamente ragionevole, avendo avuto riguardo, appunto, alla totalità delle circostanze.

---

134 *R. v. Cole*, 2012 SCC 53; per un commento sia concesso rinviare a F. GIOVANELLA, *Immagini pedopornografiche, privacy del lavoratore e protezione costituzionale: il punto della Corte Suprema canadese*, in *Il Diritto dell'Informazione e dell'Informatica*, 2013, 34.

135 Section 24(2): "Where […] a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute".

136 *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253. Si trattava anche in questo caso di detenzione di materiale pedopornografico. Durante un intervento presso l'abitazione di Morelli, un tecnico del provider si insospettì per la presenza sul computer di quest'ultimo di alcuni link con nomi eloquenti, di una telecamera puntata sulla sala da gioco del figlio e di videocassette con e senza etichetta. Il sospetto incrementò quando, tornato il giorno seguente per completare le operazioni di manutenzione della rete, il tecnico trovò la casa in ordine, il computer formattato, e la telecamera puntata altrove. Denunciò l'accaduto ad un'agenzia per la protezione dei minori, che a sua volta contattò la polizia, la quale richiese ad un giudice di pace un mandato per poter ispezionare l'abitazione di Morelli.

137 *R. v. Morelli*, cit., parr. 105-106.

138 *R. v. Cole*, cit., par. 34-35.

139 [1996] 1 S.C.R. 128 (S.C.C.).

Dato che si trattava di informazioni contenute nel disco fisso del computer e di file Internet, ciò che veniva in rilievo era l'*informational privacy*, intesa come diritto di un individuo a determinare per sé quando, come e in che modo, informazioni che lo riguardano siano comunicate ad altri (punto 1)[140]. L'interesse diretto dell'imputato era desumibile, secondo i giudici canadesi, dal fatto stesso che egli utilizzasse il computer per navigare in Internet e per conservare informazioni personali (punto 2). Dai punti 1 e 2 conseguiva implicitamente una aspettativa soggettiva del ricorrente (punto 3), che doveva però essere valutata quanto a ragionevolezza avendo riguardo alla "totalità delle circostanze". A parere della Corte più il materiale oggetto di ispezione è vicino al nucleo intimo delle informazioni personali, più ciò incide sulla ragionevolezza dell'aspettativa di privacy. L'aspettativa di privacy deve essere valutata alla luce di ciò che altri soggetti, trovandosi nella medesima posizione, riterrebbero ragionevole (punto 4).
Occorreva valutare la realtà operativa del luogo di lavoro di Cole: l'analisi evidenziava sia indici nel senso dell'esistenza di un'aspettativa ragionevole (perché le regole interne alla scuola permettevano all'imputato di utilizzare il computer per uso personale) sia nel senso dell'inesistenza di tale aspettativa (perché sia le *policy* del luogo di lavoro sia la tecnologia privavano l'imputato del controllo e dell'accesso esclusivi alle informazioni contenute nel *pc*)[141]. Tenendo dunque a mente la totalità delle circostanze, da un lato la natura delle informazioni in gioco e l'utilizzo personale del computer spingevano per il riconoscimento di un interesse alla privacy, e dall'altro l'appartenenza del computer all'istituto, le *policy* e le pratiche del luogo di lavoro, nonché la tecnologia, spingevano nel senso contrario. Di conseguenza, secondo la Corte Suprema vi era una aspettativa di privacy, per quanto affievolita e l'ispezione effettuata dalla polizia era dunque illecita, né poteva venire in rilievo l'intervenuto consenso del terzo/datore di lavoro[142]. Ciò infatti significherebbe permettere che la privacy di un individuo possa essere nella disponibilità di un terzo, con ciò facendo venir meno le garanzie di cui alla Section 8[143]. Un tale approccio entrerebbe peraltro in contrasto con i principi cardine della privacy nel sistema canadese, fra cui spicca appunto il consenso dell'interessato, che dev'essere informato e liberamente dato, nonché fondato su sufficienti informazioni necessarie al fine di una scelta consapevole[144]. La teoria del consenso del terzi entrerebbe anche in collisione con la qualificazione del diritto alla privacy come diritto fondamentale protetto costituzionalmente[145].
La sentenza *R. v. Cole* ha segnato un punto di svolta della giurisprudenza canadese sull'aspettativa di privacy (lavorativa): essa rende chiaro che le policy aziendali non annullano l'aspettativa di privacy del dipendente e, anzi, possono concorrere a determinarla[146]. Questa decisione ha avuto e continua ad avere effetti dirompenti sulla

[140] La corte canadese cita testualmente A. WESTIN, *Privacy and Freedom*, New York, 1967, 7.
[141] *R. v. Cole*, cit., par. 49-54.
[142] La Corte, nella sua decisione, chiarisce che questa dottrina è applicata con autorevolezza negli Stati Uniti (citando i seguenti casi: *United States v. Matlock*, 415 U.S. 164 (U.S. Sup. Ct. 1974); *Illinois v. Rodriguez*, 497 U.S. 177 (U.S. Sup. Ct. 1990)), ma la rigetta così come aveva già fatto in passato: v. R. *v. Sanelli*, [1990] 1 S.C.R. 30 (S.C.C.) e *R. v. Wong*, [1990] 3 S.C.R. 36 (S.C.C.).
[143] *R. v. Cole*, cit., par. 73-74.
[144] *R. v. Cole*, cit., par. 77-78.
[145] Si perdoni il rinvio a F. GIOVANELLA, *Copyright and Information Privacy: Conflicting Rights in Balance*, Cheltenham, 2017, 144 ss.
[146] *R. v. Cole*, cit., par. 53.

giurisprudenza relativa alla privacy dei lavoratori, anche nelle controversie decise con *grievance arbitration* fra sindacati e datori di lavoro[147], nelle quali in verità già in precedenza il diritto alla privacy sul luogo di lavoro era stato riconosciuto[148].

Il caso *Saskatchewan Government and General Employees Union (SGEU) v. Unifor Local 481* riguardava un licenziamento a supporto del quale il datore di lavoro aveva prodotto delle *e-mail*[149]. In difesa del lavoratore, il sindacato sosteneva che le *e-mail* non fossero ammissibili perché raccolte in violazione dell'aspettativa di riservatezza del dipendente. Il datore di lavoro allegava che le policy interne alla società chiarivano che i dipendenti non potevano avere alcuna riservatezza[150]. Il sindacato poneva l'accento sul forte impatto della sentenza *R. v. Cole*: anche quando gli strumenti sottoposti a ispezione sono di proprietà datoriale, non si estingue l'aspettativa di privacy del lavoratore, soprattutto se le informazioni sono significative, intime e collegate strettamente con il "biographical core" del soggetto interessato[151]. Nel caso di specie, le policy interne permettevano l'utilizzo della rete aziendale per scopi personali purché tale utilizzo non fosse in contrasto con il lavoro del dipendente e non fosse esplicitamente proibito dalle stesse policy. Il fatto che il sistema informatico fosse di proprietà del datore di lavoro era un fattore di cui tenere conto, ma non poteva di per sé far venire meno l'aspettativa di privacy dei dipendenti.

Nell'adottare la propria decisione, l'arbitro applicava un test ricavato dalla giurisprudenza precedente[152], basato sulle seguenti domande: "1) was it reasonable, in all the circumstances, to request a surveillance; 2) was the surveillance conducted in a reasonable manner; and 3) were there other alternatives open to the company to obtain the evidence it sought"[153].

Le policy aziendali chiarivano che i lavoratori non dovevano aspettarsi riservatezza e che il datore aveva il diritto di accedere al sistema e accertare i contenuti dei file; al contempo le policy prevedevano un eventuale uso "incidentale" della posta elettronica per motivi personali che non era né esplicitamente vietato né esplicitamene approvato, e che comunque non doveva interferire con il lavoro del dipendente o di altri[154]. Se per un verso le policy aziendali riducevano grandemente l'aspettativa di privacy dei dipendenti, quest'ultima non scompariva, anche in ragione del fatto che oggigiorno non è realistico

147 V. ad esempio un caso di ispezioni sul luogo di lavoro (*Agrium Vanscoy Potash Operations and United Steelworkers Local 7552 (2015) SLAA No. 1 (Norman)*) e una controversia relativa all'utilizzo di email lavorative per scopi personali (*Department of Education v. Canadian Union of Public Employees (2014) NBQB No. 034*). già in precedenza sia in sede arbitrale sia giurisprudenziale il diritto alla privacy sul luogo di lavoro era stato riconosciuto

148 Si considerino un caso relativo all'utilizzo dei poligrafi: (*Loomis Armored Carth Service and Independent Canadian Transit Union (1997) 70 LAC (4) 400 (Kelleher)*); una controversia relativa a riprese video non autorizzate (*Brewer's Retail Inc. and United Brewers' Warehousing Workers' Union (1999) 78 LAC (4) 394 (Herman)*), un procedimento per utilizzo di cani anti-droga (*R. v. Kang-Brown (2008) 1 SCR 456*).

149 *Re Saskatchewan Government and General Employee Union and Unifor Local 481* 2015 CanLII 28482 (SK LA).

150 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pag. 2.

151 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pag. 8. Il riferimento è alla nota sentenza della Corte Suprema canadese nel caso *R. v. Plant*, [1993] 3 S.C.R. 281, 293: "it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".

152 *Doman Forest Products and IWA Local 1357* (1990) 13 LAC (4) 275 (Vickers).

153 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pag. 15.

154 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pag. 15

pensare che un dipendente non utilizzi per motivi personali la rete aziendale, la posta elettronica o un qualunque altro strumento lavorativo utile a comunicare (cellulare, computer, tablet...). La linea che separa il tempo di lavoro dal tempo non lavorativo è ormai spesso sfumata[155]. Come chiarito anche dalla Corte Suprema in *Cole* le policy interne non possono essere determinanti nel definire l'aspettativa di privacy di un lavoratore[156]: ciò non significa che un datore non possa mai esaminare le *e-mail* di un dipendente, anche se personali, significa piuttosto che il datore deve attenersi al test sopra riportato e che, dunque l'ispezione dovrà essere, sotto tutti gli aspetti, ragionevole. Considerato che è inevitabile che l'*e-mail* siano utilizzate anche a scopi personali e considerato che le email tra coniugi sono evidentemente connotate da maggiore riservatezza, l'ispezione effettuata dal datore non era da considerarsi legittima[157].

In un caso più recente, il licenziamento del dipendente Ahmar Khan era conseguito alla lettura dei suoi messaggi personali sui profili Twitter e WhatsApp effettuata attraverso un computer condiviso, sul quale il lavoratore non aveva effettuato il "log-out"[158]. Egli sosteneva di avere un'aspettativa di privacy sul computer e su tali messaggi, anche in ragione del contratto collettivo che prevedeva all'articolo 1 che i dipendenti avessero il diritto a lavorare in un ambiente rispettoso della loro privacy[159]. La Canadian Broadcasting Corporation, società datrice, riteneva invece che trattandosi di computer di lavoro e per giunta condiviso, il dipendente non potesse vantare un'aspettativa di privacy[160]. L'arbitro cui era devoluta la decisione si rifece alla sentenza *Cole* e sottolineò che, oltre al fatto che la CBC permetteva l'utilizzo dei computer lavorativi per scopi personali anche se limitati, la tipologia di lavoro di Khan, giornalista, in qualche modo richiedeva l'utilizzo di social networks e dunque non poteva considerarsi anomalo che si avvalesse di un pc di lavoro ancorché condiviso, per fare uso di tali piattaforme[161]. Sebbene possano esservi delle ipotesi in cui la ricerca, la lettura e la condivisione di messaggi personali possano giustificarsi, come nel caso di procedimenti penali, nel caso di Khan non v'era questo tipo di giustificazione: i dipendenti che avevano utilizzato il computer successivamente, avrebbero dovuto effettuare il *log-out* e non, invece, cercare i messaggi e condividerli con gli amministratori della società datrice. In aggiunta, la previsione specifica contenuta nel contratto collettivo del diritto ad avere un ambiente di lavoro in cui sia garantita riservatezza doveva essere letta come un impegno serio a raggiungere tale obiettivo, oltre a quanto già statuito da *statutory law* e *common law*[162]. Per queste ragioni la privacy del dipendente doveva indubbiamente considerarsi violata, con conseguente diritto a ottenere un risarcimento dei danni subiti[163].

Dalla disamina che precede emerge il cambiamento di rotta causato dalla sentenza della Corte Suprema *R. v. Cole*, che caratterizza il sistema canadese nel senso di un

155 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pagg. 22-23.
156 *R. v. Cole*, cit., par. 53.
157 *Re Saskatchewan Government and General Employee Union and Unifor Local 481*, cit., pagg. 23-26.
158 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, 2021 CanLII 761 (CA LA), 1-22.
159 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, cit., 17; 31.
160 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, cit., 22.
161 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, cit., 29.
162 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, cit., 30-31.
163 *Re Canadian Broadcasting Corporation and Canadian Media Guild*, cit., 41.

riconoscimento ampio e concreto di un'aspettativa di riservatezza anche in capo al lavoratore che abbia agito scorrettamente. Questo orientamento si pone in contrasto con quello molto meno garantista che connota invece il sistema USA.

IV. Gli interventi della Corte Europea dei Diritti dell'Uomo

La Corte EDU si è confrontata con il tema qui di interesse nei casi *Halford v. UK*[164], *Copland v. UK*[165], *Bărbulescu v. Romania*[166], *Garamukanwa v. UK*[167]: tutte le controversie ruotano attorno all'applicazione dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo, ovverosia la norma a tutela del "Diritto al rispetto della vita privata e familiare" che, come noto, grazie a un costante sforzo interpretativo espansivo effettuato dalla Corte EDU, copre situazioni fra loro molto diversificate fra cui entra a pieno titolo anche la riservatezza del lavoratore dipendente[168].

Il caso *Halford v. UK* deciso nel 1997 riguardava Alison Halford, un'agente di polizia che nel 1983 assunse il ruolo più alto in grado per una donna poliziotto in tutto il Regno Unito. Per anni la donna provò a progredire in carriera, ma le sue richieste furono sempre respinte. Certa che ciò dipendesse da una questione di genere, la donna promosse un procedimento per discriminazione contro il suo superiore e contro il corpo di polizia presso cui lavorava. In conseguenza alla sua azione giudiziaria, la poliziotta divenne bersaglio di mobbing da parte di molti colleghi, fino a un procedimento disciplinare per una presunta negligenza professionale, seguita da un'escalation di eventi che portarono l'agente a chiudere il rapporto di lavoro nel corso del 1992[169].

Halford aveva un ufficio con due telefoni, uno dei quali per uso privato; la poliziotta non aveva avuto istruzioni sull'utilizzo dei telefoni, i quali non erano sottoposti a restrizioni. L'agente sosteneva che i telefoni fossero stati sottoposti a intercettazione con lo scopo di ottenere informazioni da usare contro di lei nel procedimento per discriminazione. Di conseguenza presentò ricorso all'*Interception of Communications Tribunal*, il quale la informò che non era in grado di specificare se vi fossero state intercettazioni[170].

In virtù del fatto che al tempo gli individui non potevano accedere direttamente alla Corte EDU, Halford si rivolse alla *European Commission of Human Rights*, sostenendo che le intercettazioni telefoniche subite costituissero violazione del suo diritto al rispetto della vita privata e famigliare *ex* art. 8 della Convenzione[171]. La Corte ritenne che, anche sulla base della propria giurisprudenza, le comunicazioni effettuate da Halford, sia dall'ufficio, sia da casa, ricadessero sotto la protezione dell'art. 8[172]. La poliziotta poteva vantare una

---

164 App. n. 20605/92, 25 giugno 1997.
165 App. n. 62617/00, 3 aprile 2007.
166 App. n. 61496/08, 5 settembre 2017.
167 App. n. 70573/17, 6 giugno 2019.
168 Per un commento approfondito dell'art. 8 della Convenzione v. W.A. Schabas, *The European Convention on Human Rights: A Commentary*, Oxford, 2016, 358 ss.; European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, 2024, reperibile all'url: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.
169 *Halford v. UK*, cit., parr. 8-15.
170 *Halford v. UK*, cit., parr. 16-20.
171 Halford sostenne che vi fosse anche la violazione della sua libertà di manifestazione del pensiero (art. 10) e che fosse stata discriminata sulla base del genere (art. 14, in combinato con gli artt. 8 e 10); cfr. *Halford v. UK*, cit., parr. 38-39.
172 *Halford v. UK*, cit., parr. 43-44.

ragionevole aspettativa di privacy in quanto non le era mai stato detto che le comunicazioni avrebbero potuto essere intercettate; in aggiunta l'ufficio era di suo uso esclusivo e uno dei due telefoni ivi collocati era inteso per uso privato. Halford aveva tra l'altro avuto rassicurazioni scritte sulla possibilità di utilizzare il telefono per comunicazioni relative al suo procedimento per discriminazione. Queste ragioni portarono al Corte a ritenere che le telefonate dell'agente ricadessero nelle nozioni di "vita privata" e di "corrispondenza" di cui all'art. 8[173]. La Corte era inoltre dello stesso avviso della Commissione riguardo al fatto che si fossero verificate delle intercettazioni sulle telefonate effettuate dall'agente nel suo ufficio: tali interferenze non potevano essere considerate "in accordance with the law" ai sensi dell'art. 8 della Convenzione, in quanto nessuna norma interna al Regno Unito si occupava di fornire una protezione adeguata in contesti simili[174]. Conseguentemente la Corte ritenne che si fosse verificata una violazione dell'art. 8.

Il successivo caso *Copland v. UK*, riguardava Lynette Copland che era stata assistente personale del "College Principal" del Carmarthenshire College dal 1991 al 1995 e successivamente assistente del "Deputy Principal" dello stesso *college*[175]. Il telefono, le *e-mail* e la rete Internet utilizzati da Copland erano soggetti a monitoraggio su richiesta del Deputy Principal, al fine di accertare che la dipendente non facesse uso eccessivo degli strumenti lavorativi per scopi personali[176]. Il monitoraggio si limitava all'analisi dei dati dell'uso del telefono (es. destinatari delle telefonate, data e ora, durata…) e dei dati relativi all'uso di Internet (es. siti visitati, data e ora, durata…). Copland venne dapprima a sapere che il suo utilizzo della posta elettronica era sottoposto a indagine e successivamente fu informata da altri colleghi che fra il 1996 a il 1999 molte delle sue attività erano state monitorate dal Deputy Principal o da suoi delegati[177]. Al tempo non vi era alcuna *policy* interna al luogo di lavoro che riguardasse il monitoraggio dell'uso del telefono, dell'*e-mail* e di Internet da parte dei dipendenti[178].

A differenza del caso *Halford* sopra analizzato, nel caso della signora Copland non vi erano state intercettazioni sul contenuto delle chiamate o delle *e-mail* o del web, ma soltanto l'analisi dei dati relativi all'utilizzo di tali strumenti[179].

Copland riteneva che il monitoraggio dovesse comunque considerarsi un'interferenza con la sua vita privata, così come emergeva dall'adozione – successiva ai fatti di causa – da parte del Regno Unito di alcune normative che riconoscevano tali condotte come violazioni dell'art. 8[180]. Il College non aveva espressamente un potere di sorvegliare i dipendenti e le prerogative che gli competevano per legge non rendevano la sorveglianza

[173] *Halford v. UK*, cit., parr. 45-46.
[174] *Halford v. UK*, cit., parr. 48-51.
[175] *Copland v. UK*, cit., parr. 1-8.
[176] *Copland v. UK*, cit., par. 10.
[177] *Copland v. UK*, cit., parr. 11-13.
[178] *Copland v. UK*, cit., parr. 15-18.
[179] Il Governo del Regno Unito riteneva in ogni caso che tale monitoraggio, anche qualora ritenuto un'interferenza con la vita privata tutelata dall'art. 8, fosse giustificato per proteggere i diritti e le libertà altrui, in particolare per assicurarsi che ci fosse un abuso di strumenti di un datore di lavoro finanziato con denaro pubblico; in tal senso il monitoraggio era da considerarsi proporzionato e legittimo in una società democratica, v. *Copland v. UK*, cit., parr. 32-35.
[180] Il riferimento è alla Regulation of Investigatory Powers Act 2000 e alla Telecommunications (Lawful Business Practice) Regulation 2000; cfr. *Copland v. UK*, cit., par. 20.

ragionevolmente prevedibile. Inoltre, secondo Copland, il datore di lavoro avrebbe potuto utilizzare metodi meno intrusivi per comprendere quale fosse l'utilizzo degli strumenti da parte dei lavoratori, come ad esempio divulgare delle chiare policy interne[181].

La Corte, sulla scorta della propria giurisprudenza precedente, ritenne le chiamate effettuate dal luogo di lavoro erano coperte dalla nozione di "vita privata" e di "corrispondenza" di cui all'art. 8 e che lo stesso doveva ritenersi per le *e-mail* e per l'utilizzo di Internet. Considerato che Copland non aveva avuto alcuna informativa sulla possibilità che ci fosse un monitoraggio, tutte le sue attività dovevano considerarsi coperte da aspettativa di privacy. Anche se il monitoraggio riguardava solo le informazioni "esteriori" delle comunicazioni effettuate dalla ricorrente, l'art. 8 era applicabile: poco importava che le informazioni fossero state ottenute mediante le fatture, si trattava comunque di un'interferenza ingiustificata col diritto alla vita privata della donna, per cui il Regno Unito fu condannato al risarcimento[182].

Più di recente la Corte di Strasburgo ha avuto modo di affrontare la questione dell'aspettativa di privacy in relazione all'utilizzo di strumenti più moderni, come le *chat*[183].

Bogdan Mihai Bărbulescu era stato dipendente di una società romena dal 2004 al 2007. Su incarico dal suo datore di lavoro, allo scopo di rispondere alle richieste di informazioni dei clienti aveva creato un account Yahoo Messenger col quale comunicare in tempo reale con i clienti.

Le *policy* aziendali vietavano l'uso personale di computer, fotocopiatrici, telefoni e fax, ma non specificavano nulla in merito a eventuali monitoraggi dei lavoratori. Bărbulescu risultava essere stato informato di queste *policy*, avendone firmata una copia nel dicembre 2006.

Il 3 luglio 2007 il datore di lavoro faceva circolare una lettera in cui ribadiva il divieto di utilizzare Internet, telefono e fax per motivi extra-lavorativi e specificava che la condotta dei dipendenti sarebbe stata monitorata e se necessario punita[184]. Bărbulescu firmava tale lettera in un momento compreso fra il 3 e il 13 luglio, giorno nel quale il datore di lavoro informava Bărbulescu che le sue comunicazioni erano state monitorate e che risultava che avesse usato Internet per scopi personali. Egli negava di aver mai usato Yahoo Messenger per scopi personali, ma lo stesso giorno gli veniva consegnato un fascicolo di 45 pagine che riportava la trascrizione dei messaggi, alcuni con contenuti intimi e personali, che aveva scambiato mediante Yahoo Messenger con la sua fidanzata e il fratello. Il dipendente ribatté al proprio datore che violare il segreto sulla corrispondenza era reato e il 1° agosto dello stesso anno fu licenziato[185].

Il lavoratore impugnò il licenziamento chiedendo anche un risarcimento del danno patrimoniale e non patrimoniale: le corti rumene decisero in favore del datore di lavoro in

181 *Copland v. UK*, cit., parr. 37-38,
182 *Copland v. UK*, cit., parr. 41-49.
183 Mi riferisco a Bărbulescu v. Romania, cit.; per un commento si v. F. BUFFA, *Il controllo datoriale delle comunicazioni elettroniche del lavoratore dopo la sentenza Bărbulescu 2 della Cedu*, in *Questione Giustizia*, 18 ottobre 2017; A. AMBROSINO, *Riflessioni sul potere datoriale di controllo alla luce delle pronunce della Corte europea dei diritti dell'uomo sul caso Bărbulescu c. Romania*, in *Variazioni sui Temi del Diritto del Lavoro*, 2018, 257 ss.
184 La lettera portava l'esempio di una lavoratrice che era stata licenziata per l'utilizzo illecito di internet: cfr. *Bărbulescu v. Romania*, cit., par. *15*.
185 *Bărbulescu v. Romania*, cit., parr. 11-23.

quanto egli ha diritto di supervisionare e monitorare i dipendenti, soprattutto se sospetta che vi siano attività pericolose per l'azienda. Secondo le corti interne per verificare il comportamento di Bărbulescu il datore non aveva altra alternativa se non quella di controllare il contenuto delle comunicazioni, dato che il dipendente aveva negato di aver utilizzato lo strumento per scopi personali. Le corti rumene, dunque, ritennero che vi fosse un giusto bilanciamento fra gli interessi del datore e la protezione della riservatezza del dipendente e che il licenziamento fosse legittimo in quanto il comportamento di Bărbulescu integrava grave inadempimento[186].

Bărbulescu si rivolse alla Corte EDU ritenendo che ci fosse stata una violazione dell'art. 8, facendo leva tra gli altri sul caso *Copland* e quindi sostenendo che le comunicazioni telefoniche e le *e-mail* dal luogo di lavoro sono da considerarsi coperte dalla nozione di "vita privata"[187].

Il caso fu deciso in prima battuta il 12 gennaio 2016 dalla Sezione Quarta della Corte EDU, la quale ritenne che non si potesse parlare di una violazione dell'art. 8 in quanto le policy interne proibivano categoricamente l'utilizzo dei computers dell'azienda per scopi personali; in ciò il caso di Bărbulescu differiva dai precedenti *Copland* e *Halford*. Infatti, il datore di lavoro aveva avuto accesso alle comunicazioni solo dopo che il dipendente aveva comunicato di aver utilizzato Yahoo Messenger per scopi non lavorativi. La Sezione Quarta qualificò il comportamento di Bărbulescu come illecito disciplinare e, dato che le corti rumene per giungere alle loro decisioni non avevano utilizzato i contenuti delle comunicazioni del dipendente, era giunta alla conclusione che non vi fosse stata alcuna violazione dell'art. 8 della Convenzione.

Il caso fu portato davanti alla *Grand Chamber* la quale osservò che gli scambi di messaggi con Yahoo Messenger erano sicuramente da considerare comunicazioni ai sensi dell'art. 8 e che come tali rientravano nella nozione di corrispondenza anche se inviati da un computer aziendale[188].

Al fine di decidere il caso, la Corte elencò alcuni fattori da tenere in considerazione: 1. se il dipendente sia stato informato della possibilità che il datore lo monitori e quali sono le modalità e il contenuto dell'informativa; 2. l'entità del monitoraggio effettuato e il grado di intrusione nella riservatezza del lavoratore; 3. se il datore abbia o meno fornito delle ragioni legittime che giustificassero il monitoraggio e l'accesso al contenuto delle comunicazioni; 4. se sarebbe stato possibile utilizzare metodi di monitoraggio meno intrusivi; 5. le conseguenze subite dal lavoratore che è stato sottoposto al monitoraggio e l'uso che il datore ha fatto dei risultati; 6. se il dipendente avesse idonee garanzie, soprattutto quando il monitoraggio sia stato intrusivo. Sarà poi necessario che a

[186] *Bărbulescu v. Romania*, cit., parr. 24-31. Le corti rumene avevano riferimento alle norme interne: la Costituzione agli articoli 26 e 28 protegge rispettivamente la vita privata e familiare e le comunicazioni postali, conversazione telefoniche ad altre forme di comunicazione, che sono definite "inviolabili"; . Al contempo, il Codice del lavoro prevede al suo articolo 40 che il datore ha diritto a supervisionare in che modo i dipendenti espletino le loro funzioni e ha l'onere di garantire la confidenzialità dei loro dati personali. V. *Bărbulescu v. Romania*, cit., par. 35.

[187] *Bărbulescu v. Romania*, cit., par. 25.

[188] *Bărbulescu v. Romania*, cit., parr. 71-81.

disposizione del dipendente vi siano dei rimedi giudiziali dove una corte possa valutare tali fattori[189].

Nel caso di specie le corti rumene non avevano valutato se Bărbulescu fosse o meno stato informato in anticipo della possibilità che vi fosse un monitoraggio, né avevano vagliato le modalità di monitoraggio e l'entità e il grado di intrusione subito dal dipendente. Nelle decisioni delle corti interne non vi era inoltre alcun riferimento alle ragioni giustificatrici del monitoraggio in quanto il lavoratore non aveva esposto la società datrice ad alcun rischio concreto, al più i rischi erano teorici. Per tutte queste ragioni, la Corte EDU ritenne che vi fosse stata una violazione dell'art. 8[190].

In un successivo caso deciso dalla Corte EDU nel corso del 2019, *Garamukanwa vs. UK*, il ricorrente era stato licenziato dal suo datore di lavoro perché colpevole di aver inviato ai colleghi *e-mail* anonime dal contenuto riprovevole, soprattutto a una collega con cui aveva in precedenza avuto una relazione. La donna aveva denunciato Garamukanwa per *stalking* e molestie: le indagini della polizia, che arrestò l'uomo, si basarono tra l'altro su fotografie e altri materiali contenuti nel suo *smartphone*; tali materiali furono passati dalla polizia al datore di lavoro di Garamukanwa, che inizialmente sospese il dipendente. Successivamente vi fu un'audizione in cui il lavoratore fornì al suo datore alcune comunicazioni personali quali *e-mail* e messaggi WhatsApp fra lui e la sua collega con cui aveva avuto una relazione. Sulla base di queste informazioni e di quelle fornitegli dalla polizia, il datore di lavoro lo licenziò. Durante il procedimento contro il licenziamento, Garamukanwa sostenne che il datore avesse violato l'art. 8 della CEDU perché aveva fondato il licenziamento su informazioni private e personali e non aveva fatto distinzioni fra le informazioni "pubbliche" (come le *e-mail* inviate a tutti i colleghi) e informazioni "private" (quali le comunicazioni *e-mail* e WhatsApp fra lui e la sua ex fidanzata). Le corti interne ritennero che Garamukanwa non godesse di una ragionevole aspettativa di privacy sul materiale utilizzato dal datore di lavoro per procedere al licenziamento; in ogni caso, anche qualora fosse stato applicabile l'art. 8 della Carta, la compressione dei diritti del dipendente era giustificata dalla necessità di proteggere la salute e il benessere degli altri lavoratori[191].

La Corte EDU partendo dal presupposto che anche le comunicazioni lavorative possono essere considerate "corrispondenza", purché vi sia una aspettativa di *privacy* sottolinea come tale fattore, pur essendo significativo, non è determinante[192]. Nel caso di specie, il ricorrente sapeva, prima ancora delle indagini delle polizia e, dunque, ben prima del licenziamento, che la sua *ex* fidanzata aveva sollevato la questione che i suoi comportamenti fossero molesti e che il suo datore di lavoro considerasse tali comportamenti inappropriati. Pertanto Garamukanwa non poteva vantare alcuna aspettativa di privacy: in questo infatti si distingue dal caso *Bărbulescu*, in quanto in

189 *Bărbulescu v. Romania*, cit., parr. 121-122.
190 *Bărbulescu v. Romania*, cit., parr. 133-141.
191 *Garamukanwa vs. UK*, cit., parr. 1-13.
192 *Garamukanwa vs. UK*, cit., par. 22, citando *Bărbulescu v. Romania*, cit., par. 73.

quest'ultimo il dipendente non era stato in alcun modo informato circa le attività di monitoraggio da parte del suo datore[193].

V. UN CONFRONTO FRA GLI APPROCCI SOTTO LA LENTE "ITALIANA"

Dal raffronto fra gli approcci sopra descritti emerge piuttosto chiaramente un diverso modo di operare e di intendere la ragionevole aspettativa di privacy del lavoratore. Tali diversità sottendono una concezione differente di un concetto apparentemente uguale e, soprattutto, sono frutto di un bilanciamento fra interessi e diritti che sfocia in risultati spesso diametralmente opposti pur partendo dai medesimi dati.

Il sistema statunitense applica il test duale introdotto da *Katz v. US* anche nel contesto lavorativo, chiedendosi 1) qual è l'uso che l'individuo fa dello strumento di lavoro e cioè quale sia l'aspettativa soggettiva di privacy, e 2) qual è la conoscenza da parte del dipendente delle *policy* adottate dal dator e dunque se sia una aspettativa che i consociati considererebbero ragionevole. La stragrande maggioranza dei casi analizzati dimostrano come il ruolo chiave sia giocato dalle *policy*: l'esistenza stessa delle policy e la loro se non conoscenza quantomeno conoscibilità azzera l'aspettativa o la rende irragionevole. Questa interpretazione è evidente nel confronto fra i casi *United States v. Simons* e *Leventhal v. Knapek*, dove una situazione pressoché identica è risolta in maniera antitetica proprio sulla base del contenuto e della conoscenza delle policy aziendali[194]. Né vi sono particolari differenze fra lavoro pubblico e lavoro privato: pur non applicandosi il 4° emendamento, il *tort of intrusion upon seclusion* non se ne discosta significativamente in termini pratici. Molto spesso non esiste alcuna aspettativa di privacy: la c.d. *third-party doctrine* la esclude ogni qualvolta un dato sia fornito a un terzo, circostanza che nel contesto attuale di un mondo sempre connesso si verifica costantemente. A ciò si aggiunge la possibilità che il datore di lavoro possa acconsentire a ispezioni e perquisizioni, riducendo ulteriormente l'aspettativa di privacy del lavoratore.

Distanti dallo scenario statunitense e più vicini fra loro sembrano invece gli approcci seguiti nel sistema canadese e dalla Corte EDU. Più precisamente, si è assistito a un cambio di rotta nella giurisprudenza canadese a partire dal caso *R. v. Cole*, a seguito del quale le ipotesi di riconoscimento di una aspettativa di privacy a favore del lavoratore sono incrementate. Anche nel sistema canadese si dà rilevanza alle consuetudini e alle politiche aziendali, ma non necessariamente la presenza di policy azzera l'aspettativa di riservatezza, soprattutto quando si tratti di informazioni personali legate al "biographical core" del dipendente.

La Corte EDU è andata allargando le maglie dell'art. 8 della Convenzione, includendo sempre più fattispecie anche legate al mondo del lavoro. La Corte è arrivata a riconoscere

[193] Addirittura, durante il proprio procedimento disciplinare, Garamukanwa offrì personalmente al proprio datore alcune comunicazioni private, facendo venire meno totalmente la propria aspettativa di riservatezza. *Garamukanwa vs. UK*, cit., parr. 26-29.
La Corte EDU ha deciso altri casi che coinvolgono l'aspettativa di privacy dei dipendenti (v. in particolare *López Ribalda and Others v. Spagna*, App. n. 1874/13 e 8567/13, 9 gennaio 2018; decisa successivamente anche dalla Grand Chamber in data 17 ottobre 2019; *Köpke v. Germania*, app. 420/07, 5 ottobre 2010); tuttavia si ritiene di non trattare tali casi in questo contributo in quanto non riguardano la sorveglianza degli strumenti di lavoro, bensì la sorveglianza degli ambienti e delle persone dei lavoratori.

[194] V. *supra* par. 2.1.

un'aspettativa di privacy anche nelle informazioni relative alle comunicazioni senza che necessariamente ci fosse un'intromissione nel contenuto. I diversi casi decisi dai giudici di Strasburgo denotano, ancora una volta, la centralità delle policy aziendali conosciute o conoscibili dai dipendenti, che costituiscono in tutti i sistemi analizzati il vero perno della questione. La differenza sta nella concreta valutazione della conoscenza delle policy e della loro legittimità: nel sistema USA la mera conoscibilità delle policy azzera automaticamente l'aspettativa del lavoratore a prescindere dal contenuto delle policy stesse, mentre negli altri due sistemi considerati si dà maggior peso alla concreta conoscenza delle policy e al loro contenuto.

Come si è avuto modo di anticipare in apertura, nell'ordinamento italiano non si rinviene il concetto di aspettativa di privacy e di primo acchito parrebbe una figura difficilmente inquadrabile secondo le norme italiane in materia di privacy e protezione dei dati personali nel contesto lavorativo. Tuttavia, si può forse tentare una analogia fra il concetto fin qui analizzato e l'istituto dei c.d. "controlli difensivi". Si tratta di una peculiare applicazione dell'art. 4 dello Statuto dei lavoratori[195] relativo a "Impianti audiovisivi e altri strumenti di controllo". Come noto, tale articolo vieta il controllo a distanza dei lavoratori mediante strumenti che siano impiegati per ragioni organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale, se non preceduto da idoneo accordo con le rappresentanze sindacali. Nella sua attuale formulazione[196], il co. 2 dell'art. 4 prevede che il divieto cui si è appena accennato "non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"[197]. Infine, il co. 3 sancisce che le informazioni raccolte ai sensi dei precedenti commi sono utilizzabili "a tutti i fini connessi al rapporto di lavoro" purché al dipendente sia stata data "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196", meglio noto come "Codice della privacy".

Con una giurisprudenza piuttosto creativa, che continua nel solco già tracciato in passato anche dopo le modifiche intervenute negli ultimi anni[198], nel tentativo di allentare il divieto di cui all'art. 4 la Corte di cassazione ha elaborato nel tempo un concetto particolare che è appunto quello dei controlli difensivi: al datore di lavoro è riconosciuto un potere di controllo particolarmente ampio se si tratta di verificare la commissione di atti illeciti da parte di un dipendente[199]. In sostanza il datore ben può sorvegliare il dipendente qualora

195 Che come noto è la L. 20 maggio 1970, n. 300.

196 Risultante dalle modifiche intervenute con il d.lgs. 151 del 14 settembre 2015, art. 23, co. 1.

197 Cfr. M.T. SALIMBENI, *Art. 4 L. 20 maggio 1970, n. 300*, in R. DE LUCA TAMAJO, O. MAZZOTTA (a cura di), *Commentario breve alle leggi sul lavoro*, Padova, 2018, 819-820. Non appare sempre agevole distinguere quali siano tali strumenti, cfr. P. TULLINI, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?*, in P. TULLINI (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, Torino, 2017, 104; V. MAIO, *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011*, *ivi*, 75 e ss.

198 V. G. CASSANO, *Quando il giudizio di proporzionalità salva i controlli difensivi occulti: Corte europea dei diritti dell'uomo e Corte di Cassazione a confronto*, in *Diritto delle relazioni industriali*, 2022, 544 ss.; M. MARAZZA, *I controlli a distanza del lavoratore di natura "difensiva"*, in P. TULLINI (a cura di), Controlli a distanza e tutela dei dati personali del lavoratore, cit., 27 ss. Fra le più recenti sentenze della Corte di cassazione: Cass., Sez. Lav., 26 giugno 2023, 18168, in *Mass. Giur. Lavoro*, 2023, 614 con nota di M. ROSA; 12 novembre 2021, n. 34092, in *Giust. Civ. Massimario*, 2021; 22 settembre 2021, n. 25732, in *Diritto delle Relazioni Industriali*, 2022, 271.

199 M.V. BELLESTRERO, G. DE SIMONE, *Diritto del lavoro*, Torino, 2022, 378. Non è questa la sede per illustrare diffusamente questa discussa interpretazione giurisprudenziale, anche a seguito delle novità

nutra il sospetto della commissione di atti illeciti; ciò si pone però in contrasto con l'art. 4 medesimo, soprattutto se non sono rispettate le condizioni dettate dall'articolo stesso, fra cui il rendere edotto il lavoratore della possibile sorveglianza[200].

Questa sorveglianza, che si basa in sostanza su controlli occulti, seppure successivi alla scoperta dell'attività illecita[201], somiglia in tutto e per tutto alle situazioni da cui scaturiscono le controversie più sopra illustrate, in cui si rinviene il concetto di ragionevole aspettativa di privacy. Sarà invero determinante che il lavoratore sappia di poter essere sottoposto a monitoraggio e sia in condizione di comprendere ciò che può e non può fare quando esegue le proprie mansioni, e in che termini ed entro che limiti la sua prestazione possa essere oggetto di controllo[202].

Tuttavia la giurisprudenza della Cassazione, pur tenendo bene a mente i precedenti della Corte EDU, non arriva a ritenere la comunicazione preventiva elemento necessario al fine della legittimità del controllo difensivo, ma si limita e ritenerlo solo uno degli elementi utili a orientare il bilanciamento del giudice italiano[203]. Il giudice italiano deve bilanciare i diritti e gli interessi in gioco, applicando una serie di fattori, considerando determinati indici ed elementi utili, esattamente come le corti dei sistemi qui analizzati fanno nelle ipotesi di ragionevole aspettativa di privacy.

È stato sottolineato che dare eccessiva importanza all'informativa finisca di fatto non solo per escludere qualunque controllo occulto[204], ma anche per legittimare qualunque controllo, seppur manchevole dei requisiti di cui all'art. 4, co. 1. Valorizzare eccessivamente il co. 3 vorrebbe dire mettere nelle mani del datore di lavoro uno strumento potentissimo di elusione delle regole di cui all'art. 4, con l'aggravante che

introdotte negli ultimi anni; si rinvia pertanto fra i molti a A. BELLAVISTA, *Il controllo sui lavoratori*, Torino, 1995; E. GRAGNOLI, *L'informazione nel rapporto di lavoro*, Torino, 1996; A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, 2013; V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Argomenti di diritto del lavoro*, 2015, 1186; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro*, 2016, I, 77, C. ZOLI, *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970*, in *Variazioni su Temi di Diritto del Lavoro*, 2016, 635 ss.

Con riferimento in particolare ai controlli difensivi e alle "nuove tecnologie" si v. R. IMPERIALI, R. IMPERIALI, *Controlli sul lavoratore e tecnologie*, Milano, 2012, spec. 173 ss.; A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, 2013, spec. 91 ss.

200 A. RICCOBONO, *Nuove tecnologie e controlli difensivi tra diritto positivo e creazionismo giudiziario*, in *Rivista Italiana di Diritto del Lavoro*, 2023, I, 514-515.

201 A. RICCOBONO, *Nuove tecnologie e controlli difensivi tra diritto positivo e creazionismo giudiziario*, cit., 517 ss.

202 A. RICCOBONO, *Nuove tecnologie e controlli difensivi tra diritto positivo e creazionismo giudiziario*, cit., 523.

203 Per un raffronto fra approccio della Cassazione italiana e Corte EDU v. G. CASSANO, *Quando il giudizio di proporzionalità salva i controlli difensivi occulti: Corte europea dei diritti dell'uomo e Corte di Cassazione a confronto*, cit.; L. TEBANO, *Employees' privacy and employers' control between the Italian legal system and European sources*, *Labour & Law Issues*, 2017, C. 3.

204 V. MAIO, *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011*, cit., 75.

l'informativa è un atto unilaterale datoriale[205], che si inserisce in rapporto notoriamente connotato da una asimmetria difficilmente superabile[206].
Questo scenario si avvicinerebbe molto a quello statunitense dove, come visto, la conoscenza delle policy aziendali azzera qualunque aspettativa di privacy.
Da questo rapido raffronto si evince come, sebbene il concetto di aspettativa di privacy non sia riscontrabile in senso stretto nel nostro ordinamento, la giurisprudenza sui controlli difensivi può esservi accostata.

VI. CONCLUSIONI

Il presente scritto ha preso le mosse dal concetto di "ragionevole aspettativa di privacy" elaborato nel contesto dell'applicazione del 4° emendamento della Costituzione americana e ne ha indagato portata e peculiarità nel rapporto di lavoro. Lo studio è stato circoscritto alle ipotesi di violazione della riservatezza del lavoratore per il tramite degli strumenti di lavoro e, in particolare, mediante il monitoraggio dell'utilizzo di telefoni, computer e altri strumenti simili. Si è visto come l'approccio statunitense si dimostri quello meno garantista, essendo di fatto sufficiente la conoscenza delle policy aziendali da parte del lavoratore per scardinare qualunque aspettativa di privacy dello stesso, sia in ambito pubblico che in ambito privato. Invero, sebbene nei due contesti si applichino norme diverse, ovverosia il 4° emendamento nel pubblico e il *tort of inclusion upon seclusion* nel privato, l'aspettativa di privacy entra sempre in gioco e la sua ragionevolezza è facilmente scalzata dall'introduzione di policy aziendali.
Gli approcci canadese e della Corte EDU sembrano offrire maggiore tutela al lavoratore. In Canada, il cambio di rotta verificatosi con la sentenza *R. v. Cole* ha determinato l'imporsi di un'interpretazione più favorevole al dipendente, dove l'aspettativa di privacy persiste anche in presenza di policy chiare e conosciute dal lavoratore, specie quando a entrare in gioco siano informazioni vicine al c.d. "biographical core". La giurisprudenza della Corte di Strasburgo dà a sua volta molta importanza alla conoscenza delle consuetudini e delle regole aziendali, ma le considera solo uno fattori da valutare per determinare l'aspettativa del lavoratore.
Queste differenti prospettive sono state poi poste a confronto con l'ordinamento italiano, dove, sebbene l'aspettativa di privacy non sia contemplata formalmente, è possibile rinvenire un equivalente funzionale nella disciplina dei controlli difensivi.
In conclusione si può pertanto riscontrare da un lato l'avvicinarsi degli strumenti utilizzati dalle corti per dirimere le controversie relative alla sorveglianza (degli strumenti) del lavoratore, dall'altro l'allontanarsi delle soluzioni proposte nei vari ordinamenti. In questo senso, il caso studio qui presentato dimostra ancora una volta la divergenza, già nota alla

[205] G. CASSANO, *Quando il giudizio di proporzionalità salva i controlli difensivi occulti: Corte europea dei diritti dell'uomo e Corte di Cassazione a confronto*, cit., 547-548. Sull'informativa v. A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 24-25; v. già GRUPPO ART. 29, *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*, WP 55, 29 maggio 2002, 14-15.
[206] V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, cit., 1215 sottolinea la criticità dell'aver portato sul piano del rapporto datore/lavoratore l'equilibrio che prima era posto a livello collettivo.

letteratura[207], fra la disciplina di privacy e protezione dei dati personali nel contesto statunitense da un lato e nei contesti europeo e canadese dall'altro.

[207] Sia concesso rinviare a F. GIOVANELLA, *Copyright and Information Privacy: Conflicting Rights in Balance*, cit. e alla dottrina *ivi* citata.

TUTELA DELLA PROPRIETÀ INTELLETTUALE NEL MONDO DELL'INTELLIGENZA ARTIFICIALE: ARTIFICIAL INVENTOR PROJECT, THALER E I BREVETTI NEGATI A DABUS*

Isabella Ferrari

SOMMARIO:

This paper presents reflections against the suitability of introducing a new category of subjective personality, headed by AI systems, based on the analysis of a legal experiment initiated on a global scale within the framework of Thaler's so-called Artificial Intelligence Project.
This stance is predicated upon a comprehensive analysis of the technical components of AI systems and their legal implications within the context of the regulatory framework introduced by the European Union. This framework encompasses the Artificial Intelligence Act (proposal), the Data Act, the Data Governance Act and its associated guidelines, the Digital Services Act, and the Digital Markets Act (proposal).

Keywords: intelligenza artificiale; Thaler; Dabus; data-set.

I. DAL DIVIETO DI INTERESSE ALLA PRESENZA DELLA *SHARIA'H* NELL'ECONOMIA

Tutela della proprietà intellettuale ed intelligenza artificiale afferiscono a due mondi distinti e separati, talora persino confliggenti.
Ché infatti la tutela intellettuale mira a proteggere la creatività umana, ovverosia il frutto del lavoro, dell'impegno e dell'intelligenza personali.
Di contro, l'intelligenza artificiale si avvale del lavoro pregresso altrui, per imparare ed acquisire quella formazione, necessaria per restituire all'utente risposte rimodulate a partire dallo scibile originariamente introdotto nel sistema.
Non a caso i software di intelligenza artificiale sono correntemente definiti sistemi di *machine learning*, a sottolineare la particolare modalità di assimilazione massiva di conoscenze, su cui si fonda l'operatività algoritmica[1].
Prima facie, l'intelligenza artificiale parrebbe allora essere un semplice ausilio per indagini documentali, analisi statistiche e raccolte di dati. Già tale utilizzo, per quanto strumentale, apre comunque a potenzialità enormi: basti pensare alle ricerche innovative, rese possibili dalla capacità intrinseca dell'intelligenza artificiale di ricollegare informazioni

* Il presente contributo è un prodotto della ricerca svolta nell'ambito del progetto "Intellectual property protection for Industry 4.0" (n. 101085321 Erasmus-2022), finanziato dall'Unione Europea, di cui l'Autrice è *Principal Investigator*. Le opinioni espresse appartengono, tuttavia, alla sola Autrice e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

[1] Il *machine learning* si fonda anche e soprattutto sull'aggregazione a lungo termine dei dati personali, con ovvie ripercussioni in tema di potenziali problemi di privacy, come rilevato *ex multis* dalla Corte Suprema degli Stati Uniti in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018), su cui anche E. Nicolella, *Evolving Privacy Protections for Emerging Machine Learning Data under Carpenter v. United States,* in *FIU Law Review*, 2023, 17(2), pp. 453-478. Anche il Garante per la protezione dei dati personali italiano è intervenuto ripetutamente in materia, sottolineando la necessità in caso di violazioni digitali della privacy, di adottare tutte le misure necessarie a mitigare gli esiti e gli impatti diretti, incluse le notificazioni alle vittime delle violazioni medesime: si richiamano tra i tanti provvedimenti, i nn. 173, 194 e 196 del Registro dei provvedimenti del Garante Privacy italiano del 21 marzo 2024.

apparentemente sconnesse, trovando chiavi di lettura e di indagine, invisibili alla mente umana. Vi sono poi applicazioni digitali e sistemi IoT che pervadono ogni aspetto della nostra quotidianità[2], permettendoci di rintracciare rapidamente prodotti, luoghi, dati e informazioni, a prescindere dalla loro collocazione spazio-temporale.
Insomma, i programmi che si avvalgono dell'intelligenza artificiale riescono a vagliare ed esaminare con assoluta precisione ed accuratezza miriadi di dati digitali, per fornire nell'immediato risultati, se non esatti, quanto meno attendibili ed affidabili.
I sopradescritti utilizzi presuppongono tuttavia sempre la presenza di un agente umano, che, al pari di quanto fa il pittore col pennello, utilizza l'intelligenza artificiale come strumento nelle sue mani, per velocizzare e migliorare la sua attività, che è e resta pur sempre un'attività umana.
Lo sviluppo tecnologico ci ha però posti dinnanzi ad una nuova tipologia di intelligenza artificiale, sempre più evoluta, capace di allenarsi su un pacchetto di dati selezionato in ingresso dall'uomo, e di costruirne via via uno più ampio in completa autonomia: si tratta della cd. intelligenza artificiale generativa[3].
La peculiarità di questa versione avanzata dell'intelligenza artificiale risiede allora, prima ancora che nelle sue specificità operative, nel data-set di funzionamento, ovverosia nel bagaglio di informazioni digitali, che costituisce il sostrato necessario per l'operatività del sistema: data-set che si espande ed accresce esponenzialmente nell'uso ripetuto nel tempo. Come dire che alla base dell'intelligenza artificiale generativa non vi è esclusivamente l'algoritmo operativo, ma anche e soprattutto un data-set auto-generato e generante, che muta, si accresce e si specializza da solo[4].
Ne consegue l'inadeguatezza dei tradizionali approcci giuridico-normativi nel regolare i sistemi di intelligenza artificiale generativa, dal momento che essi sogliono considerare esclusivamente la stringa algoritmica, mentre trascurano perlopiù il data-set di riferimento[5], su cui il sistema si forma ed allena.
A ben guardare, pertanto, l'affidabilità e la sicurezza dell'intelligenza artificiale impongono un approccio duale, che valuti paritariamente algoritmo e dati, giacché entrambi sono elementi imprescindibili per il funzionamento del sistema nel suo complesso, ed entrambi sono meritevoli della medesima attenzione normativa e regolatoria.

---

[2] Cd. *Internet of Things*, ovverosia l'organizzazione di un sistema connesso di oggetti che raccolgono, trasmettono e analizzano dati al fine di automatizzare un'operazione o un'azione in molteplici settori, incluso quello industriale, aziendale, domestico e di ricerca. Per una trattazione tecnica della materia si rinvia *ex multis* a C. S. Hutchinson, *Curbing Big Tech's IoT dominance,* in *European Competition Journal*, 2022, 18(2), p. 265–266; K. Goldstein, *Cyber Beware: IOT Technology Growing Explosively,* in *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel*, 2019, 3(6), p. 8 (l'Autore definisce IoT come un "concetto di connessione" di un dispositivo a Internet e ad altri dispositivi connessi, diretto a raccogliere e scambiare dati tramite sensori incorporati nel dispositivo medesimo).

[3] Per una definizione di intelligenza artificiale generativa, si rinvia a H.H. Perritt Jr., *Copyright for Robots?,* in *Indiana Law Review*, 2023, 57(1), p. 143; H.H. Perritt Jr., *Robot Slanderer,* in *University of Arkansas at Little Rock Law Review*, 2023, 46(2), pp. 169-236; J.M. Garon, *The Revolution Will Be Digitized: General AI, Synthetic Media, and the Medium of Disruption*, in *Ohio State Technology Law Journal*, 2023, 20(1), pp. 139-223.

[4] S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Ed. Laterza, Bari, 2004; V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (eds.) *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, pp. 23-59.

[5] Le decisioni emesse in tal senso afferiscono per lo più al settore pubblicistico, come dimostra la sent. 10964/2019 Tar Lazio, sez. III bis, che censura la spersonalizzazione del processo decisionale, come a dire che il software operi unicamente sulla base di parametri matematico-statistici, senza previa formazione ed allenamento sulla base delle decisioni pregresse su casi analoghi. I. Forgione, *Il caso dell'accesso al software Miur per l'assegnazione dei docenti (Nota a TAR Lazio, sez. III bis, 14 febbraio 2017, n. 3769),* in *Giornale di diritto amministrativo*, 2018, 5, p. 647; M.C. Cavallaro, G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo,* in *Federalismi.It*, 2019, 16, pp. 1-22.

II.. LA TUTELA DELLA PROPRIETÀ INTELLETTUALE NEL PRISMA DELL'INTELLIGENZA ARTIFICIALE

La proprietà intellettuale artificiale va diversamente considerata e valutata in ragione del differente grado di autonomia di ciascun sistema algoritmico.

Nell'ipotesi in cui il sistema di intelligenza artificiale venga impiegato quale mero strumento per facilitare o agevolare il lavoro umano, *nulla quaestio*: l'invenzione resta cioè ascrivibile all'uomo, anche quando quest'ultimo si sia avvalso di sistemi algoritmici in fase di ricerca e sviluppo[6].

Diverso è invece il caso dell'intelligenza artificiale generativa, per la quale occorre domandarsi se la scintilla creativa sia effettivamente umana o artificiale[7].

Va da sé che, in base ad un approccio strettamente e rigidamente eziologico, se un'invenzione è generata in completa autonomia da un sistema algoritmico, allora quest'ultimo dovrebbe esserne ritenuto l'inventore, con tutte le conseguenze giuridiche che ne conseguono sul piano della tutela della proprietà intellettuale. Si tratterebbe tuttavia di un esercizio di antropomorfizzazione fine a se stesso, inidoneo a tutelare in concreto l'inventore e i consumatori finali. Ché, infatti, la riconduzione dell'inventorialità artificiale entro categorie ed archetipi tipicamente umani, finirebbe per negare la straordinarietà della fattispecie. Come dire che ricondurre l'intelligenza artificiale generativa nell'alveo della tradizionale tutela intellettuale, equivarrebbe a piegare la realtà entro i confini degli inquadramenti giuridici classici. Ma l'intelligenza artificiale generativa, specie quando è auto condotta e capace di decidere in autonomia quali compiti svolgere e di cosa occuparsi, rappresenta un elemento dirompente, che stravolge integralmente la realtà.

Mentre sono ancora ben lontani gli inquietanti scenari transumanisti e di singolarità tecnologica[8], occorre tuttavia prendere atto della eccezionalità della materia, che richiede necessariamente una trattazione giuridica del tutto nuova. Non resta allora che abbandonare gli schemi e i modelli classici del diritto tradizionale, per riconsiderare la questione della protezione intellettuale artificiale su basi del tutto diverse, ferma tuttavia la garanzia di tutela di tutti i soggetti coinvolti, da legare causalmente ai programmatori.

III. CREATIVITÀ E BREVETTABILITÀ

La proprietà intellettuale gode della protezione in diritto solo se risultano soddisfatti in concreto i tre requisiti della novità, originalità e applicabilità industriale. Siffatti requisiti, elaborati in seno alla *civil law*, ancorché diversamente declinati nei sistemi giuridici contemporanei (nella *common law* statunitense il riferimento è ai concetti di novità, non

[6] L'impiego strumentale dell'intelligenza artificiale spazia dal settore medico-sanitario (si pensi al fulmineo progresso scientifico registrato grazie all'impiego di sistemi d'intelligenza artificiale in occasione della ricerca vaccinale per contrastare la pandemia da Covid-19), a quello ingegneristico (che copre gli ambiti edile, manufatturiero, della mobilità, ecc.), a quello sociale ed ambientale (per studiare i flussi e predire i comportamenti).

[7] Sulla distinzione tra tecnologie di supporto e tecnologie sostitutive, cfr. E. Calzolaio, *Intelligenza artificiale ed autonomia della decisione: problemi e sfide*, in E. Calzolaio (ed.) *La decisione nel prisma dell'intelligenza artificiale*, Cedam, Padova, 2020 pp. 3-4. Si rinvia anche a N.F. Frattari, *Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale,* in *Contr. impr.*, 2020, p. 469, che distingue tra macchine intelligenti che eseguono le istruzioni ricevute, quelle impostate teleologicamente nel loro funzionamento, e quelle capaci di *self-learning.*

[8] Seppur talora prospettati dai critici dell'intelligenza artificiale, come in C. D. Cummings, *Transhumanism: Morality and Law at the Frontier of the Human Condition,* in *Ave Maria Law Review*, 2022, 20, p. 216.

ovvietà e utilità)[9], evidenziano il significato e lo scopo ultimo della tutela della proprietà intellettuale, ovverosia la promozione dell'innovazione nell'interesse sociale e collettivo[10]. Godono infatti di tutela esclusivamente quelle invenzioni innovative che siano capaci di incrementare competitività e originalità nel settore di riferimento, permettendo l'avanzamento e il miglioramento dell'intero comparto produttivo.
Nel contesto della protezione della proprietà intellettuale per l'intelligenza artificiale, occorre allora richiamare le origini dell'istituto brevettuale per come si è sviluppato in chiave comparata nel diritto moderno e contemporaneo.
Ché infatti, dopo un avvio a macchia di leopardo, a partire dalla Magna Grecia, il concetto della tutela intellettuale si è affermato dapprima nella Firenze rinascimentale, con Brunelleschi e Leonardo da Vinci, per poi estendersi nei secoli XV-XVIII alla Repubblica di Venezia e ai Regni di Francia e Inghilterra[11]. L'evoluzione storica di questo istituto è stata quanto mai ondivaga, in un difficile bilanciamento tra la tutela privatistica ed esclusiva del soggetto inventore e, di contro, la protezione del pubblico interesse alla libera conoscenza e al libero utilizzo dei ritrovati, funzionali al progresso dello stato dell'arte[12].
Per l'effetto, la regolamentazione tecnica ha assunto due direzioni alternative ed antitetiche[13]: all'approccio teso a porre l'idea inventiva a fondamento della tutela della proprietà intellettuale, si è contrapposto quello incentrato sul meccanismo delle rivendicazioni.
Nel primo caso occorre una descrizione precisa, puntuale e dettagliata dell'invenzione per cui si chiede il brevetto, da impostare come soluzione tecnica ad un problema concreto e specifico, mentre nel secondo caso l'oggetto della tutela si ricava per sottrazione, escludendo tutto ciò che non è espressamente indicato ed opposto ai terzi[14].
Inizialmente, l'adesione all'uno o all'altro di questi due approcci ha coinciso con l'appartenenza alla famiglia di *civil* o a quella di *common law*: ché, infatti, mentre la domanda brevettuale in *civil law* doveva essere suffragata dalla ricostruzione dell'idea inventiva di

[9] J. Pagenberg, *The WIPO Patent Harmonization Treaty*, in *AIPLA Quarterly Journal*, 1991, 1, pp. 1-23; F. Gurry, *Current WIPO Developments in Copyright, Patent and Trademark Law*, in *International Intellectual Property Law & Policy*, 1996, 1, pp. 35-44.

[10] La funzione del brevetto, che è legata allo stimolo dell'innovazione, è subordinata all'efficacia costitutiva del titolo. La protezione si ottiene mettendo l'invenzione a disposizione del pubblico attraverso l'atto di pubblicazione. Per un ulteriore approfondimento, si veda G. Floridia, *Il diritto al brevetto*, in P. Auteri, G. Floridia, V. Mangini, G. Olivieri, M. Ricolfi, P. Spada (a cura di) *Diritto Industriale. Proprietà intellettuale e concorrenza*, Giappichelli, Torino, 2012, p. 245 ss.

[11] Sul ruolo dei brevetti a partire dall'economia veneziana, si veda C.A.C. Gonzalez, M.G.C. Elorza, *Review of the International Patent System: From the Venice Statute to Free Trade Agreements,* in *Mexican Law Review*, 2020, 3, pp. 65-100; P.J. Federico, *Galileo's Patent,* in *Journal of the Patent Office Society*, 1962, 8(12), pp. 576-580; S.A. Rabinowe, *Authorising the Printed Image in Early Modern Venice,* in *Art Antiquity and Law*, 2016, 21(2), pp. 157-176. Per una panoramica in chiave comparata invece dello sviluppo storico dei brevetti, si rinvia a W.R. Lane, *Patent Law,* in *Journal of the Patent Office Society*, 1960, 42(12), pp. 849-858; C.A. Nard, A.P. Morriss, *Constitutionalizing Patents: From Venice to Philadelphia,* in *Review of Law and Economics,* 2006, 2, pp. 223-322; R.A. Klitzke, *Historical Background of the English Patent Law,* in *Journal of the Patent Office Society*, 1959, 41(9), p. 635.

[12] Nel dualismo instaurato in materia di tutela della proprietà intellettuale tra i sistemi europei e statunitense, si sono di recente inseriti i sistemi giuridici cinesi, indiani, latinoamericani e africani, come rilevato in un interessante contributo di G. Marini, *Diritto e politica. La costruzione delle tradizioni giuridiche nell'epoca della globalizzazione,* in *Pòlemos*, 2010, 1, p. 31 e ss.

[13] Sulle opposte funzioni del brevetto come scopo (tutela dell'inventore) o come mezzo (incentivo allo sviluppo delle tecniche), si rinvia all'interessante analisi di J. Brinkhof, *Balancing a Fair Protection for the Patentee and a Reasonable Degree of Certainty for Third Parties*, in *International Intellectual Property Law & Policy*, 2002, 7, p. 3.

[14] *EMI v. Lissen* (1939) 56 R.P.C., p. 23. La funzione delle rivendicazioni è quella di definire in modo chiaro e preciso il monopolio rivendicato, in modo che gli altri possano conoscerne i confini esatti. Il loro scopo principale è quello di limitare gli ambiti della tutela di cui gode l'inventore, nel senso che tutto ciò che non è rivendicato cade nel pubblico dominio.

base[15], in *common law* occorreva tracciare con chiarezza e precisione i confini della tutela legale attraverso le rivendicazioni, da considerare parte integrante della domanda, a pena di nullità.

Si richiamano sul punto le disposizioni di cui al Regio Decreto italiano n. 1127 del 29 giugno 1939 sulle invenzioni industriali[16], che concentrano l'attenzione sull'invenzione brevettata, da descrivere così dettagliatamente da consentire che «ogni persona esperta del ramo possa attuarla» (art. 51 Codice della proprietà industriale italiano, introdotto con D.lgs. 10 febbraio 2005, n. 3). In senso conforme anche il diritto prussiano: «In einer Anlage ist die Erfindung dergestalt zu beschreiben, daß danach die Benutzung derselben durch andere Sachverständige möglich erscheint»[17].

Le rivendicazioni, volte a definire i limiti della tutela opponibili ai terzi, hanno tuttavia continuato a rivestire un ruolo ancillare nella costruzione della tutela brevettuale di *civil law* sino alla riforma di cui alla Convenzione di Monaco e al Trattato WIPO[18].

Si deve infatti all'art. 69 CBE e all'art. 6 PCT l'espressa ed uniforme indicazione delle rivendicazioni tra gli elementi costitutivi della domanda di brevetto; rivendicazioni da articolare in maniera chiara e concisa, così da definire con precisione l'oggetto per cui viene invocata la protezione brevettuale[19].

La contrapposizione originaria tra *civil* e *common law,* ovverosia tra sistemi che fondano il brevetto sull'idea inventiva (*civil law*) e sistemi basati sul meccanismo delle rivendicazioni (*common law*), é stata così superata dal sistema della tutela brevettuale basata sulle rivendicazioni.

Tanto che le rivendicazioni trovano ora espressa menzione nell'articolo 52, II comma del codice della proprietà industriale italiano[20], nei §§ 14 e 38 del *Patentgesetz* 1981 sotto la denominazione tedesca di *Patentanspruch,* all'articolo R612-17 *Code de la propriété intellectuelle* francese in qualità di *revendications*, e all'art. 14 della *Section* 125 del *Patents Act* 1977 che regola il *claim system* nel Regno Unito.

Il meccanismo delle rivendicazioni, così delineato, è funzionale a tutelare non già l'inventore, quanto piuttosto i terzi, contro il pericolo della cristallizzazione dello stato dell'arte per effetto di concessioni brevettuali aventi effetti monopolistici.

Ma quali sono le cause di un siffatto radicale cambio di prospettiva?

In tutta evidenza, l'acquisita centralità delle rivendicazioni nel processo di costruzione della tutela brevettuale si giustifica nel repentino e straordinario progresso tecnico e tecnologico,

---

15 La Convenzione di Parigi per la Protezione della Proprietà Industriale, del 1883, poi trasfusa nell'Accordo di Strasburgo relativo alla classificazione internazionale dei brevetti del 1971[15], ha posto sul piano internazionale le basi per una tutela fondata sul riconoscimento univoco ed assoluto dell'idea inventiva. In linea cioè con l'approccio tipicamente *civillian*, la tutela brevettuale delle origini era costruita a partire dalla definizione dell'idea inventiva. Così pure nei decreti regi italiani n. 1127 del 29 giugno 1939, e n. 1411 del 25 agosto 1940. A sottolineare la centralità dell'idea inventiva nella costruzione della tutela brevettuale, si richiamano altresì le seguenti definizioni rese nell'ambito della giurisprudenza di legittimità italiana: «idea di soluzione protetta» in Cassazione civile sez. I, 20.10.2022, n.30943; «idea inventiva», «nucleo inventivo protetto o cuore dell'invenzione brevettata» in Cassazione civile sez. I, 4.1.2022, n.120.

16 Come modificato e integrato dal Regio Decreto n. 1411 del 25 agosto 1940, e dal Decreto del Presidente della Repubblica n. 849 del 26 febbraio 1968 sulla concessione di licenze obbligatorie in materia di brevetti per invenzioni industriali.

17 § 20 *Patentgesetz* 1891. Cfr. *Deutsches Reichsgesetzblatt Band* 1891, n. 12, pp. 79-90. Il codice prussiano già nel 1891 imponeva una descrizione dell'invenzione sufficientemente chiara ed accurata da permetterne l'utilizzo anche da parte di terzi, esperti del settore

18 La convenzione di Monaco del 1973 sul brevetto europeo (CBE), e il Trattato WIPO di cooperazione in materia di brevetti del 1970 (PCT).

19 L'art. 2 del Protocollo Interpretativo dell'articolo 69 CBE sollecita l'interpretazione del brevetto in chiave di equo bilanciamento tra la tutela del titolare del brevetto e la ragionevole certezza dei terzi.

20 Introdotto con D.lgs. 10 febbraio 2005, n. 30.

avviato sulla scia dei risultati del *Dartmouth Summer Research Project on Artificial Intelligence* del 1956[21]. L'avvento di calcolatori elettronici prima, e di super-computer poi, ha via via plasmato non solo l'ambito della ricerca scientifica, ma anche quello giuridico collegato: ché infatti le potenzialità crescenti di sviluppo scientifico e industriale per effetto dell'impiego di nuovi sistemi informatici hanno imposto la contestuale riduzione dell'ambito di tutela inventoriale esclusiva, per evitare la paralisi di interi comparti produttivi.

Il passaggio dalla *central* alla *peripheral definition theory* segna dunque l'acquisita e definitiva centralità delle rivendicazioni nella costruzione del brevetto, rivoluzionandone scopo, ambiti e portata. Come dire che alla centralità delle rivendicazioni corrispondono una maggior tutela dei terzi e una minor tutela dell'inventore. L'obiettivo ultimo è quello, così facendo, di stimolare la libera competizione, e conseguentemente pure l'innovazione e il progresso tecnologico.

La riforma strutturale nella concezione degli scopi e dei limiti del brevetto, occorsa negli ultimi cinquant'anni, è stata massimamente riassunta da un'illuminante sentenza recentemente emessa dalla Cassazione civile sez. I, 4.1.2022, n.120[22], che ha fotografato l'intervenuto superamento ad opera della Convenzione di Monaco dell'approccio fondato sulla *central definition theory* , ovverosia sulla descrizione meticolosa e dettagliata dell'invenzione nel suo complesso, in favore della *peripheral definition theory* , che è «fondata sulla chiara e precisa identificazione dei limiti e dei confini della protezione brevettuale, funzionali alla determinazione del perimetro della privativa , sulla base delle caratteristiche del trovato espressamente rivendicate nel testo brevettuale»[23].

Da quanto sopra risulta evidente che l'intelligenza artificiale si inserisce nel contesto della tutela della proprietà intellettuale, per la sua intrinseca natura propulsiva nello sviluppo dell'Industria 4.0. Occorre tuttavia distinguere le invenzioni in ragione del diverso ruolo ricoperto dall'intelligenza artificiale all'interno del procedimento inventivo.

Nell'eventualità in cui l'intelligenza artificiale sia incorporata in un nuovo ritrovato inventivo, e ne costituisca imprescindibile ed inseparabile parte integrante[24], l'intelligenza artificiale non rileva ai fini della tutela brevettuale.

Allorché invece l'intelligenza artificiale operi come fonte autonoma e creativa del ritrovato finale, l'analisi giuridica diventa significativamente più intricata, dovendosi distinguere tra l'intelligenza artificiale generativa che opera in maniera autonoma o al contrario su istruzioni q umane.

IV. THALER E DABUS

Nella valutazione di una domanda di brevetto, occorre esaminare abstract, descrizione, rivendicazioni ed eventuali disegni tecnici.

Come dire che ogni decisione è (*rectius*, dovrebbe essere) assunta unicamente avendo riguardo al contenuto inventivo, e cioè al merito dell'invenzione.

---

21 J. Mccarthy, M. Minsky, N. Rochester, C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955. La Conferenza di Dartmouth segna la nascita dell'intelligenza artificiale. L'ipotesi discussa e validata in quella sede era che qualunque aspetto dell'apprendimento o di qualsiasi altra caratteristica dell'intelligenza umana potesse essere descritto con una tale precisione da poter essere simulato da una macchina. La Conferenza era volta a determinare come le macchine potessero essere programmate per utilizzare il linguaggio, formare astrazioni e concetti, risolvere problemi precedentemente riservati agli esseri umani e migliorare se stesse nel tempo.

22 Rivista di Diritto Industriale 2022, III, p. 350.

23 In linea con l'approccio in uso nel contesto statunitense sotto il corollario della cd. *all elements rule*, in base a cui per la sussistenza della contraffazione in concreto occorre dimostrare la riproduzione di tutti gli elementi rivendicati.

24 È il caso dei software con compiti di calcolo o di analisi dei dati.

Se così fosse, nulla osterebbe a che anche un sistema di intelligenza artificiale generativa possa essere titolare di un brevetto, con tutte le conseguenze giuridiche che ne derivano (titolarità dei diritti morali e patrimoniali, responsabilità risarcitoria, ecc.). E pur tuttavia, la brevettabilità delle invenzioni artificiali è stata sin qui rifiutata in diritto.

Il diniego del riconoscimento della proprietà intellettuale artificiale si giustifica con il timore che l'enorme capacità produttiva dell'intelligenza artificiale, che si sviluppa nell'ordine di potenze infinite della creatività umana, possa portare al sovraccarico degli uffici brevetti nazionali e internazionali, determinandone l'impossibilità d'azione a fronte di una miriade di domande provenienti da inventori artificiali. Un simile accadimento porterebbe al collasso dell'intero sistema brevettuale globale, con conseguente impossibilità di ottenere tutela per qualunque nuova invenzione, artificiale o umana, e in ultima analisi determinerebbe una diffusa e deleteria paralisi innovativa e produttiva.

D'altra parte, le normative di riferimento in materia di protezione della proprietà intellettuale fanno riferimento ad inventori umani, giacché risalgono tutte a epoche in cui non era tecnicamente ipotizzabile che un elaboratore elettronico potesse agire in via autonoma[25]. Col che, nel vuoto normativo che permane sul punto, non è tuttora possibile, in diritto, riconoscere l'esistenza di un inventore artificiale.

Per sollecitare un'evoluzione giuridico-normativa, atta riconoscere l'autonoma capacità inventiva dei sistemi di intelligenza artificiale generativa, Stephen Thaler ha avviato un esperimento giuridico multidisciplinare e cross-border, nell'ambito del cd. *Artificial Inventor Project*[26].

Attraverso diciassette controversie senza scopo di lucro, avviate in diverse giurisdizioni nel mondo, il progetto di Stephen Thaler mira a promuovere il riconoscimento della proprietà intellettuale in capo all'intelligenza artificiale, in assenza di un inventore umano tradizionale.

Stephen Thaler, esperto di reti neurali artificiali, è il fondatore e amministratore delegato di *Imagination Engines*, che ha sviluppato Dabus. Dabus è l'acronimo di *Device for the Autonomous Bootstrapping of Unified Sentience*: si tratta di un programma di intelligenza artificiale composto da due reti neurali. La prima rete genera nuovi progetti di prodotti, mentre la seconda rete valuta le proposte progettuali sviluppate dalla prima rete neurale, per selezionare quelle che reputa migliori, e conseguentemente degne di essere mandate in produzione.

Attraverso un processo *up-stream*, l'essere umano è stato coinvolto esclusivamente nella fase iniziale di avviamento di Dabus, allorché è stato configurato l'algoritmo d'esecuzione del programma e sono stati selezionati gli elementi del data-set per l'alimentazione e l'addestramento del software. Poi, una volta avviato, il sistema Dabus ha operato in piena autonomia. Ciò gli ha permesso, *ex multis*, di sviluppare due prodotti finali degni di essere mandati in produzione: una fiamma neurale, che funziona come sistema di allarme per le

[25] Si vedano la Convenzione sul brevetto europeo del 1973, il Patents Act inglese del 1977, il Patentgesetz tedesco risalente al 1877 nella sua versione originaria, la legge francese sulla tutela brevettuale n. 68-1 del 2 Gennaio 1968, la legge sul diritto d'autore n. 633/1941 e il Codice della Proprietà Industriale introdotto in Italia dal Decr.Lgs. 30/2005, ecc. Cfr. G. Resta, *Decreto legislativo 10 febbraio 2005, n. 30, Codice della proprietà industriale*, in A. Barba, S. Pagliantini (eds.) *Commentario del Codice Civile. Delle Persone*, Utet, Torino, 2013, pp. 163-198; A. Venchiarutti, *Das italienische Gesetzbuch für das gewerbliche Eigentum - Codice della Proprietà Industriale Italiano*, Giappichelli, Torino, 2017; A. Somma, *Diritto comparato e rivoluzione*, in *Rechtsgeschichte Legal History*, 2013, pp. 198-202; A. Somma, *Il diritto della Rivoluzione Industriale*, in *Rechtsgeschichte Legal History*, 2016, pp. 473-480.

[26] R. Abbott, *The Reasonable Robot. Artificial Intelligence and the Law*, Cambridge University Press, Cambridge, 2020: questo studio esamina la finora incontestata neutralità giuridica dell'intelligenza artificiale e analizza la questione con riferimento al principio di trasparenza e causalità. L'obiettivo dichiarato dell'Artificial Inventor Project è quello di promuovere il dialogo sull'impatto sociale, economico e legale delle nuove tecnologie. Inoltre, mira a generare una guida per gli stakeholder sulla proteggibilità dei prodotti generati dall'IA.

luci di emergenza, e un contenitore per alimenti in plastica creato con l'uso della geometria frattale.
Per questi due prodotti, Stephen Thaler ha presentato domanda di brevetto a nome di Dabus presso diciotto uffici nel mondo, e specificatamente presso l'ufficio brevetti australiano, inglese, europeo, statunitense, tedesco, israeliano, coreano, giapponese, neozelandese, cinese, canadese, taiwanese, brasiliano, indiano, sudarabico, di Singapore, svizzero e sudafricano.
In tutte le richieste brevettuali depositate, Dabus è stato indicato quale titolare dei diritti morali sul prodotto inventivo, e Stephen Thaler quale titolare dei connessi diritti patrimoniali[27]. Tuttavia, tutti gli uffici, eccetto quello sudafricano, hanno respinto le domande di Thaler, innescandone la reazione giudiziaria in via di impugnazione.
Solo una parte dei procedimenti sono stati definiti in ultima istanza, mentre la gran parte del contenzioso è ad oggi ancora *sub judice*. Allo stato attuale, nessuna corte interpellata ha riconosciuto la brevettabilità delle invenzioni di Dabus, e non già per carenza nel merito del contenuto inventivo, bensì per mancanza di un inventore umano.
L'analisi della storia procedurale dei casi Dabus offre interessanti spunti di riflessione giuridica[28].

V. Breve excursus sulle controversie promosse da Stephen Thaler per conto di Dabus

Il 29 luglio 2019, Stephen Thaler ha depositato presso l'U.S. Patent and Trademark Office (USPTO) due domande di brevetto intestate a Dabus, l'una relativa alla luce neurale e l'altra al contenitore per alimenti sviluppato tramite geometria frattale, di cui sopra[29].
In base alla legge federale statunitense, le domande di brevetto devono essere corredate dalla dichiarazione di autenticità della relativa invenzione. Tuttavia, poiché Dabus non poteva fornire una simile dichiarazione personale, Stephen Thaler ha dichiarato l'autenticità delle due invenzioni *de quibus*, identificandosi contestualmente in qualità di rappresentante legale di Dabus (e perciò autorizzato a delegare terzi a rendere la dichiarazione di autenticità) e delegato da Dabus a rendere la dichiarazione di autenticità[30].
Lo USPTO ha però ritenuto inammissibile la dichiarazione resa da Stephen Thaler, siccome agente nella duplice veste di delegato e delegante, e ha respinto entrambe le domande di brevetto depositate da Dabus, per loro manifesta incompletezza in punto alla necessaria dichiarazione d'autenticità, censurando altresì (*ad abundantiam*) la mancata indicazione di un inventore umano.
Stephen Thaler ha impugnato il diniego dello USPTO innanzi la Corte distrettuale della Virginia orientale, che, oltre a confermare in via definitiva la decisione amministrativa di rigetto del brevetto, ha ampliato il *petitum*. Ché infatti in sede giudiziaria, la discussione non è stata confinata alla validità o invalidità della dichiarazione di autenticità allegata da Thaler (su cui lo USPTO aveva fondato il proprio diniego), ma ha coinvolto il tema centrale del

[27] Nella giurisprudenza in materia di brevetti, mai è accaduto che un procedimento fosse attuato contra se, ovverosia per ottenere il riconoscimento del brevetto in favore di altri. Cfr. J. Goodman, *Homography of Inventorship: DABUS and Valuing Inventors,* in *Duke L & Tech Rev*, 2021-2022, 20, p. 1 ss.
[28] F. Vessia, *Riflessioni sulla brevettabilità delle «invenzioni computazionali» a margine del caso DABUS,* in *AIDA*, 2023, pp. 365-388; A. Amidei, *Quale tutela per l'opera generata dall'A.I.? Il nostro diritto d'autore è troppo "antropomorfo"?,* in *Italian Legal Tech Report*, 2024, Giuffrè, Milano, pp. 40-46.
[29] U.S. Patent Application No. 16/524,350. Cfr. S. Bora Cinar, *Intellectual Property Law's Test with DABUS: Can Artificial Intelligence Systems Be Recognised as Inventors?,* in *Inonu University Law Review*, 2023, 14(2), pp. 387-400; J. Millamena, *How Artificial Intelligence Machines Can Legally Become Inventors: An Examination of and Solution to the Decision on DABUS,* in *Journal of Law and Policy*, 2021, 30(1), pp. 270-304.
[30] 35 U.S.C. §115(B): «The oath or affirmation ... shall contain statements that ... such individual believes that he or she is the original inventor or an original co-inventor of an invention claimed in the application».

soggetto inventore. A tal proposito, la Corte federale statunitense ha precisato che il termine *inventor* può riferirsi unicamente alle persone fisiche, in linea coi precedenti vincolanti e con il lessico comune, e ha escluso tassativamente la possibilità di interpretazioni estensive della normativa vigente, in mancanza di un indirizzo di politica legislativa di segno contrario[31].

Come dire che la Corte statunitense ha rifiutato i brevetti richiesti da Stephen Thaler per Dabus, senza nemmeno entrare nel merito del contenuto delle invenzioni depositate, e ha rinviato ogni discussione teorico-giuridica al legislatore[32].

Anche il procedimento europeo promosso da Stephen Thaler ha avuto esito negativo per Dabus[33]. Ché infatti lo European Patent Office ha rifiutato la concessione dei due brevetti richiesti da Thaler (relativi alle due invenzioni sopra descritte, ovverosia la fiamma neurale e il contenitore per alimenti creato tramite geometria frattale) per mancanza di un inventore identificabile con una persona fisica. Impugnando il provvedimento amministrativo di diniego, Stephen Thaler ha richiamato in giudizio la sussistenza di un rapporto di lavoro tra lui e Dabus, basato sulla *hire doctrine*[34].

Per l'effetto, Stephen Thaler si è auto-qualificato cessionario dei diritti patrimoniali associati ai brevetti richiesti, alla stregua di quanto usualmente accade per le invenzioni sviluppate nell'ambito di un rapporto di lavoro, con il datore di lavoro che trattiene i diritti economico-patrimoniali a titolo di ricompensa per i pregressi investimenti in ricerca e sviluppo, e il dipendente-inventore che conserva la titolarità morale sull'opera.

Le domande di Thaler sono state però respinte tanto in primo grado, quanto in sede di appello dall'EPO, che ha fatto precedere alle motivazioni in diritto un'argomentazione tanto sintetica quanto *tranchant*:

> «A machine is not an inventor within the meaning of the EPC»[35]

L'EPO ha infatti stabilito che ai sensi e per l'effetto del combinato disposto di cui all'art. 81 e regola 19(1) della Convenzione sul brevetto europeo, l'inventore deve necessariamente essere una persona fisica. Ad ogni buon conto, l'EPO ha ritenuto irrealizzabile in concreto il trasferimento di diritti da Dabus, nella sua supposta condizione di dipendente, in favore di Stephen Thaler, quale datore di lavoro, posto che, in mancanza di personalità giuridica e di capacità d'agire, Dabus non avrebbe potuto legittimamente trasferire alcunché a terzi.

Similmente si è sviluppato anche il contenzioso inglese, dove pure si è recentemente raggiunta la *res judicata*[36].

Lo UK Intellectual Property Office ha invitato Stephen Thaler ad integrare le due domande di brevetto depositate a nome e per conto di Dabus con le necessarie dichiarazioni di autenticità dell'invenzione e con la documentazione atta dimostrare il suo

---

31 T.F. Ward, *DABUS, an Artificial Intelligence Machine, Invented Something New and Useful, but the USPTO Is Not Buying It,* in *Maine Law Review,* 2023, 75(1), pp. 71-100.

32 Decisione del 27 ottobre 2022, in *Thaler v. Iancu, et al*, 1:20-cv-00903; and *Thaler v. Vidal*, 43 F .4th 1207, 1209 (Fed. Cir. 2022). See M. Messina, *Thaler v. Vidal, 43 F .4th 1207 (F ed. Cir. 2022)*, in *DePaul J. Art, Tech. & Intell. Prop. L.*, 2023, 33, p. 67.

33 Domande depositate il 17 ottobre e il 7 novembre 2018, n. EP 18 275 163 (relativa a un contenitore per alimenti) e n. EP 18 275 174 (relativa a dispositivi e metodi per attirare maggiore attenzione), decise il 21 dicembre 2021: Caso n. J 0008/20-3.1.01; Pubblicazione n. 3564144. Cfr. M. Ricolfi, *Invenzioni e modelli di Utilità*, in (a cura di V. Di Cataldo, M. Ricolfi, M.S. Spolidoro) *I cinquant'anni della giurisprudenza annotata di diritto industriale. Passato, presente, futuro*, 2024, Giuffrè, Milano, pp. 25-51.

34 Ciò implica che l'intelligenza artificiale funzioni in modo simile a quello di un dipendente tradizionale, mantenendo la proprietà dei diritti morali associati alle proprie invenzioni. Di conseguenza, al datore di lavoro verrebbero concessi diritti di proprietà esclusivi sul ritrovato sviluppato dal dipendente inventore.

35 ECLI:EP:BA:2021:J000820.20211221.

36 *Thaler v. Comptroller-General of Patents, Designs and Trademarks*, Case No. 2021/0201; [2023] UKSC 49, (deciso con sentenza del 20 dicembre 2023), su impugnazione di [2021] EWCA Civ 1374.

presunto diritto di sfruttamento economico delle invenzioni. Stephen Thaler ha pertanto invocato la dottrina dell'accessione, che lega la proprietà dei frutti al proprietario del bene principale. Col che, auto-definendosi proprietario di Dabus, Stephen Thaler ha sostenuto di essere titolare di tutti i diritti economici sui prodotti derivati dalla creatività del sistema artificiale Dabus. Lo UKIPO ha però rigettato le richieste di brevetto *de quibus*, per incompletezza documentale, e con l'impugnazione del diniego amministrativo la questione si è spostata nelle aule di giustizia, dove sono state emesse tre decisioni conformi.

Dapprima l'High Court of Justice ha respinto l'impugnazione di Thaler, per mancanza di personalità fisica o giuridica in capo a Dabus, come richiesto invece a pena di nullità dall'Art. 7 del Patents Act 1977 per la concessione di un brevetto:

> «It is common ground that DABUS is not a person, whether natural or legal. DABUS is not a legal person because (unlike corporations) it has not had conferred upon it legal personality by operation of law. It is not a natural person because it lacks those attributes that an entity must have in order to be recognised as a person in the absence of specific (statutory) legal intervention»[37]

Poi anche la Court of Appeal[38] e la UK Supreme Court[39] hanno confermato il rigetto delle domande di Stephen Thaler e Dabus, concludendo che solo una persona fisica o giuridica può essere designata come inventore ai sensi del Patents Act del 1977. E poiché Dabus non è provvisto di capacità d'agire, non può aver validamente autorizzato Thaler né a depositare una domanda di brevetto, né tanto meno ad attestare l'autenticità delle sue invenzioni[40].

La Corte Suprema ha altresì valutato attentamente il richiamo svolto da Thaler alla dottrina dell'accessione, ritenendola tuttavia insuscettibile di applicazione rispetto alle invenzioni intellettuali.

Se infatti le invenzioni intellettuali ricevessero il medesimo trattamento giuridico riservato ai frutti materiali, allora si doterebbero di concretezza materiale.

Tuttavia, per sua stessa natura, la proprietà intellettuale non può sostanziarsi in qualcosa di tangibile: la proprietà intellettuale concerne l'idea che sta dietro e alla base di un prodotto, col che non può essere trattata secondo i canoni giuridico-interpretativi propri dei beni fisici e materiali[41].

Ne consegue la definitiva archiviazione degli approcci posti in essere da Stephen Thaler, sulla base del richiamo alla *hire doctrine*, alla teoria dell'accrescimento o all'interpretazione estensiva delle norme sul conferimento della procura legale.

È interessante osservare sul punto che mai Stephen Thaler ha proposto un riconoscimento *sic et simpliciter* di personalità giuridica o di capacità d'agire in capo all'intelligenza artificiale, né tantomeno ha ventilato la creazione di un nuovo tipo di personalità *sui generis* ad uso specifico dell'intelligenza artificiale. Una simile soluzione in diritto finirebbe evidentemente solo per spostare altrove i problemi etici e giuridici sollevati dall'avvento

---

37 High Court of Justice: [2020] EWHC 2412 (Pat), 34.

38 Court of Appeal Judgment: [2021] EWCA Civ 1374.

39 Supreme Court Judgment: [2023] UKSC 49.

40 R. Abbott, *Artificial Intelligence, Big Data and Intellectual Property: protecting computer-generated works in the United Kingdom*, in T. Aplin (ed.) *Research Handbook on Intellectual Property and Digital Technologies*, Edward Elgar Publishing, Cheltenham, 2017.

41 U. Scotti, *The intangibles. Industrial and intellectual property rights*, in *Business Law and Economics*, 2016, 1, p. 14 ss; R. Henderson, *AI and Intellectual Property Ownership: Who Is the 'Inventor' When the Machine Self-Develops?,* in *Business Law Review*, 2023, 44(3), pp. 124–125; J. Gibson, *Artificial Intelligence and Patents: DABUS and Methods for Attracting Enhanced Attention to Inventors,* in *Queen Mary Journal of Intellectual Property*, 2021, 11(4), pp. 401-408.

dell'intelligenza artificiale generativa, senza affatto prospettare soluzioni concrete né efficaci.
Di contro, Stephen Thaler ha tentato (e tenta tuttora) di ottenere un adeguamento interpretativo del diritto vigente, che consenta di plasmare e adattare le norme positive alle necessità via via emergenti nella società contemporanea, che è sempre più tecnologica e connessa.

VI. L'ILLUSIONE DI AUSTRALIA E SUD-AFRICA

Analizzando il caso Dabus all'interno del quadro giuridico australiano, emergono alcune particolari incongruenze.
Inizialmente, infatti, le domande di brevetto in favore di Dabus sono state respinte da parte del Deputy Commissioner of Patents austrialiano, per asserita incapacità dell'intelligenza artificiale di essere considerata quale soggetto inventore:

> «section 15(1) of the Patents Act 1990 (Cth) is inconsistent with an artificial intelligence system or device being treated as an inventor»[42]

Tuttavia, questa decisione è stata ribaltata dalla Federal Court of Australia, che, accogliendo integralmente le richieste di Stephen Thaler e Dabus, ha aperto ad un'interpretazione evolutiva del diritto positivo, per permetterne l'adeguamento per via giurisprudenziale in linea con l'avanzamento tecnologico[43]. In sede di appello, tuttavia, è stato riaffermato il veto australiano al riconoscimento dello status di inventore in capo ad un sistema di intelligenza artificiale, con il rigetto definitivo, ed inappellabile, delle domande di brevetto depositate da Stephen Thaler per Dabus[44]. Col che, dopo un percorso ondivago, anche il procedimento australiano si è concluso sfavorevolmente per Dabus.
L'unico ordinamento che, all'opposto, ha riconosciuto la proprietà intellettuale in capo a Dabus è stato il Sud Africa, che ha concesso i brevetti richiesti da Stephen Thaler in nome e per conto di Dabus[45].
Tuttavia, tale risultato positivo è in effetti solo parziale, dal momento che, in mancanza di un contenzioso giudiziario, che avrebbe potuto essere innescato esclusivamente a seguito del rigetto amministrativo da parte dell'ufficio brevetti competente, non è stato possibile sottoporre la questione della brevettabilità delle invenzioni artificiali al vaglio critico del diritto sudafricano. I due brevetti del Sud Africa sono stati concessi per evidenti ragioni di politica amministrativa, e cioè per affermare nel contesto globale il sostegno sudafricano all'Industria 4.0. Di conseguenza, non è dato sapere come si sarebbe potuto pronunciare un tribunale sudafricano, se la questione della titolarità brevettuale di Dabus fosse stata effettivamente affrontata e discussa in diritto[46].

---

42 Rigetto del 9 febbraio 2021 con riferimento alla domanda di brevetto n. 2019363177. Una panoramica completa del caso Dabus nel quadro giuridico australiano è fornita da R. Matulionyte, *AI as an Inventor: Has the Federal Court of Australia Erred in DABUS?, in Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2022, 13(2), pp. 99-112.
43 *Thaler v. Commissioner of Patents* [2021] FCA 879. La decisione è oggetto di un'ampia analisi in R. Kanna, P. Singh, *Thaler v Commissioner of Patents [2021] FCA 879: DABUS - an 'Inventor'?*, in *Indian Journal of Artificial Intelligence and Law*, 2022, 2, p. 11.
44 *Commissioner of Patents v. Thaler* [2022] FCAFC 62.
45 Il 28 luglio 2021, la Commissione sudafricana per le società e la proprietà intellettuale (CIPC) ha pubblicato l'accettazione del brevetto sudafricano n. 2021/03242 (brevetto SA DABUS) sul South African Patent Journal.
46 D.O. Oriakhogba, *DABUS gains territory in South Africa and Australia: revisiting the AI-inventorship question*, in *South African Intellectual Property Law Journal*, 2021, 9, pp. 87-108; D.O. Oriakhogba, *What If DABUS Came to Africa? Visiting AI Inventorship and Ownership of Patent from the Nigerian Perspective,* in *Business Law Review*, 2021, 42(2), pp. 89-99.

VII. RIFLESSIONI *DE JURE CONDENDO SULLA PROPRIETÀ INTELLETTUALE DELL'INTELLIGENZA ARTIFICIALE*

I procedimenti giudiziari avviati da Stephen Thaler per il riconoscimento della proprietà intellettuale in capo a Dabus, che è un software di intelligenza artificiale privo di personalità giuridica, hanno innescato un'interessante discussione dottrinale sul ruolo della scintilla creativa nell'ambito giuridico[47].

In altre parole, se è vero che la protezione della proprietà intellettuale ha lo scopo di tutelare le idee inventive su cui si fonda la messa in produzione di un bene su scala industriale, per incentivare ricerca e sviluppo e promuovere l'avanzamento dell'intera filiera di riferimento, allora non dovrebbe avere alcuna rilevanza la natura umana o artificiale della scintilla creativa: a prescindere cioè dal fatto che l'impulso innovativo provenga da un essere umano o da una rete neurale, in diritto dovrebbe rilevare unicamente il merito della domanda di brevetto, ovverosia il soddisfacimento in concreto dei requisiti di brevettabilità vigenti, in conformità alle regole locali.

Accade invece che in nessuno dei diciassette procedimenti giudiziari avviati da Stephen Thaler nel mondo sia stato mai esaminato il merito delle domande di brevetto: ogni corte sin qui adita ha infatti rigettato le richieste di brevetto depositate in nome e per conto di Dabus, sul presupposto della mancanza di personalità, fisica o giuridica, in capo a colui che veniva indicato come inventore, ovverosia di Dabus.

Tutte le decisioni sin qui emesse, pur nell'ambito di sistemi giuridici differenti, hanno decretato all'unanimità l'impossibilità di interpretare il diritto vigente estensivamente, per effetto di *analogia legis*, e, preso atto della lacuna normativa in tema di proprietà intellettuale artificiale, hanno rinviato la questione al formante legislativo per il necessario aggiornamento delle norme giuridiche rispetto alle nuove esigenze, emerse dallo sviluppo delle tecnologie più evolute ed innovative.

Mentre è evidente che la disciplina nazionale ed internazionale in materia di proprietà intellettuale, siccome risalente al XX secolo[48], non potesse contemplare tecnologie che all'epoca non esistevano al di fuori dei romanzi di fantascienza, ora che l'intelligenza artificiale generativa è divenuta realtà, urge disciplinarne e regolarne l'uso.

---

[47] Anche l'Ufficio brevetti tedesco ha respinto le domande di Thaler, che ha quindi impugnato la decisione davanti al Tribunale federale dei brevetti. L'11 novembre 2021, il tribunale tedesco ha confermato l'ordinanza di rigetto, sostenendo che le invenzioni generate dall'intelligenza artificiale sono brevettabili a condizione che una persona fisica sia indicata come inventore: cf. decisione in BPatG 11 W (pat) 5/21-DABUS. Per un esame del contenzioso tedesco, si rinvia a D. Kim, *The Paradox of the DABUS Judgment of the German Federal Patent Court*, in *GRUR International*, 2022, 71(12), pp. 1162-1166. Anche l'Ufficio brevetti israeliano ha rifiutato di accettare le domande di brevetto di Thaler (n. 268604 e n. 268605, depositate nel 2019 e respinte il 19 marzo 2023). La decisione è attualmente in fase di appello. Il 17 marzo 2023, anche l'Alta Corte neozelandese ha confermato il rigetto da parte del New Zealand Intellectual Property Office della domanda di brevetto di Thaler a causa dell'indicazione di DABUS quale inventore (CIV-2022-485-118 [2023] NZHC 554). Nel giugno 2023, la Corte Amministrativa di Seoul, in Corea del Sud, ha confermato la decisione dell'Ufficio della Proprietà Intellettuale sudcoreano di respingere la domanda di Thaler. In concomitanza con questa decisione, l'ufficio sudcoreano ha anche istituito un gruppo consultivo di esperti legali, tecnologici e industriali per redigere le linee guida sull'interconnessione tra intelligenza artificiale e proprietà intellettuale. Una delle questioni che il gruppo ha il compito di indagare è se la protezione della proprietà intellettuale per le invenzioni di intelligenza artificiale stimoli il progresso nel campo dell'IA. Inoltre, il gruppo consultivo ha ritenuto che non sia evidente la necessità immediata che la Corea del Sud si ponga all'avanguardia nella legislazione per consentire agli inventori che non sono persone fisiche di godere della proprietà intellettuale (Patent examination policy bureau of KIPO, White Paper on Artificial Intelligence and Intellectual Property, 2022, p. 17). Cfr. E. White, *DABUS around the World,* in *Managing Intellectual Property*, 2021, 292, pp. 12-15.

[48] Ancorché le varie norme del settore siano state aggiornate ed emendate, risalgono tutte in prima battuta alla seconda metà del '900.

Il regolamento europeo sull'intelligenza artificiale n. 2024/1684 rappresenta per certo un rilevante passo in avanti[49]. Tuttavia, la peculiare natura *a contrario* del regolamento europeo (fissa limiti e divieti in materia di intelligenza artificiale, in luogo di diritti), ed il fatto che si occupi perlopiù di intelligenza artificiale, e non già di intelligenza artificiale generativa né tantomeno di intelligenza artificiale generativa auto-decidente, non colma il vuoto normativo sul punto[50].

Stephen Thaler ha infatti sfidato le corti giudiziarie, volendole indurre a modificare il loro orientamento in materia. La sfida però non è stata raccolta pienamente dal formante giurisprudenziale, che ha invece rinviato in ultima battuta la questione al formante legislativo. Ciò in quanto l'eventuale tutela della proprietà intellettuale in capo all'intelligenza artificiale comporterebbe a cascata una serie di modifiche sostanziali in diritto: ché infatti un inventore artificiale diverrebbe titolare dei correlati diritti patrimoniali per lo sfruttamento economico del brevetto, e conseguentemente pure responsabile per eventuali danni che derivassero dai prodotti ricavati per effetto della messa in produzione del prodotto brevettato[51]. Ciò equivarrebbe in ultima analisi ad autorizzare implicitamente il riconoscimento di una nuova categoria di personalità, oltre a quella fisica e a quella giuridica: una sorta di ibrido artificiale, che renderebbe pressoché impossibile l'applicazione degli usuali canoni ermeneutici su cui si fonda la dottrina giuridica sin qui sviluppatasi nei secoli, e richiederebbe l'integrale ripensamento del diritto positivo, per come fino ad oggi è stato concepito ed applicato.

Stephen Thaler ha così evidenziato l'impellente necessità di un intervento legislativo in un settore con importanti implicazioni pratiche, economiche e politiche.

L'inquadramento giuridico delle innovazioni dell'intelligenza artificiale implica una decisione fondamentale, se cioè gli investimenti nello sviluppo dell'intelligenza artificiale generativa meritino o meno tutela legale. Al di là dei pericoli di cristallizzazione del sistema brevettuale per effetto di un sovraccarico di domande per invenzioni artificiali, occorre innanzitutto valutare se la rimodulazione dello scibile operata da un sistema di intelligenza artificiale possa o meno definirsi innovativo (e pertanto degno di tutela intellettuale).

Se è vero cioè che l'intelligenza artificiale generativa si educa e forma sulla base delle conoscenze altrui, che rielabora e rimodula in autonomia, allora le idee artificiali non dovrebbero mai dirsi originali ed innovative, dal momento che rappresentano la revisione di idee pregresse. Un simile approccio all'intelligenza artificiale generativa escluderebbe in nuce la brevettabilità delle invenzioni artificiali.

Ma, d'altronde, anche la mente umana si forma e lavora sulla base degli input e delle informazioni ricevute durante gli anni dell'educazione scolastica, universitaria, professionale, e nella vita di ogni giorno[52].

Come dire che non può essere la diversa velocità di educazione della mente umana rispetto all'intelligenza artificiale a giustificare trattamenti diversi, in diritto, per situazioni del tutto analoghe in concreto.

Gli interessi in gioco sono evidentemente tanti e consistenti, e richiedono un arduo bilanciamento[53]: occorre cioè stabilire se sia preferibile proteggere le invenzioni artificiali,

---

49 2021/0106(COD) del 21/4/2021.

50 P. BENANTI, *Oracoli. Tra algoretica e algocrazia*, Luca Sossella Editore, Roma, 2018.

51 G. Comandé, *Intelligenza artificiale e responsabilità tra «liability» e «accountability». Il carattere trasformativo dell'IA e il problema della responsabilità,* in *Analisi Giuridica dell'Economia*, 2019, 1, pp. 169-188; A. Amidei, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in U. Ruffolo (ed.), *Intelligenza Artificiale - Il Diritto, I Diritti, L'etica*, 2020, Giuffré, Milano, pp. 125-151.

52 Come sottolineato da E. Chikhaoui, S.Mehar, *Artificial Intelligence (AI) Collides with Patent Law,* in *Journal of Legal, Ethical and Regulatory Issues*, 2020, 23(2), p. 3, «Human Brains are good at Learning».

53 Come evidenziato in V. Zeno Zencovich, S. Grumbach, *A Painful Divorce: Law vs Digital Technologies,* in *European Journal Of Comparative Law And Governance*, 2024, 1, pp. 1-22, mentre i tradizionali strumenti giuridici

e con esse gli investimenti in ricerca e sviluppo tecnologico a vantaggio non solo del titolare di singoli brevetti ma anche della collettività nel suo complesso, ovvero tutelare la creatività umana, per proteggerla da un soffocante profluvio di invenzioni artificiali.
Le decisioni esaminate, tutte conformi nel negare la tutela brevettuale a Dabus, valgono ad aprire una riflessione di portata ben più vasta, in punto all'opportunità o meno dell'istituzione di una nuova categoria di soggettività in capo all'intelligenza artificiale generativa, che possa affiancarsi alle persone fisiche e a quelle giuridiche[54].
Non pare a chi scrive che sia questa la soluzione ottimale per governare in sicurezza gli sviluppi dell'intelligenza artificiale, dal momento che, al contrario, il riconoscimento di personalità (e di conseguenza pure di autonoma tutela intellettuale) in capo all'intelligenza artificiale si tradurrebbe in concreto in una grave e pericolosa fuga dalle responsabilità di coloro che programmano, allenano ed avviano i sistemi di intelligenza artificiale, garantendo loro un'inammissibile e inquietante immunità per i danni causati dall'operato dei loro prodotti.
Al fine di contenere simili derive, occorre invece ribadire che, per quanto un sistema d'intelligenza artificiale possa operare in autonomia, senza cioè che il programmatore abbia piena contezza dei meccanismi operativi e decisionali del sistema stesso, è comunque assodato che un sistema d'intelligenza artificiale opera nei limiti del data-set di riferimento e per gli effetti di cui all'algoritmo di programmazione. Come dire che il sistema d'intelligenza artificiale dà sostegno a un processo che si incardina su presupposti e su elementi scelti dall'uomo, nutrendosi, allenandosi e rielaborando esclusivamente quanto ha ricevuto in prima battuta proprio dall'uomo. Col che il sistema d'intelligenza artificiale non può sostituirsi *ex abrupto* all'essere umano: ciò non è ipotizzabile in fase di progettazione e programmazione, né tanto meno nella successiva eventuale imputazione delle responsabilità per eventuali danni che dal funzionamento dell'intelligenza artificiale possano derivare[55].
L'elemento soggettivo (dolo o colpa), indispensabile per la corretta imputazione della responsabilità, va ricollegato non già al sistema d'intelligenza artificiale, quanto invece al programmatore umano, che ha impostato l'algoritmo di funzionamento, e ha configurato il pacchetto dati con cui opera il sistema d'intelligenza artificiale.
Ebbene, sul punto occorre sottolineare che la semplice conoscenza dell'algoritmo, in totale trasparenza, non garantisce comunque la conoscenza dei metodi operativi impiegati dal

si sono dimostrati inadeguati a fronteggiare il fenomeno digitale contemporaneo, gli attori digitali sono diventati i legislatori più efficaci.

[54] Sugli agenti software, si vedano A. Azara, *Intelligenza artificiale, personalità giuridica*, in (a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto) *Il Diritto Nell'era Digitale. Persona, Mercato, Amministrazione, Giustizia*, 2022, Giuffré, Milano, p. 93 ss.; G. Sartor, *Agenti software: nuovi soggetti del ciber diritto?,* in *Contr. impr.*, 2002, p. 466 ss.

[55] Posto infatti che i qualia non appartengono all'ontologia della macchina artificiale, perché allo stato dell'arte non risulta possibile programmare un sistema d'intelligenza artificiale che comprenda e percepisca sentimenti ed emozioni[55], allora difetta alla radice un elemento ineludibile per l'allocazione in concreto della responsabilità civile, ovverosia lo stato soggettivo. L'accertamento della responsabilità civilistica postula necessariamente la sussistenza in concreto dell'elemento soggettivo, che permetta di ricollegare eziologicamente l'evento dannoso ad un fatto determinato. Ebbene, l'intelligenza artificiale sfugge dai parametri tipici di questa categorizzazione giuridica, per l'intrinseca sua incapacità di introiettare dolo o colpa nei suoi agiti. Gli aspetti qualitativi delle esperienze coscienti non possono essere tradotti in un linguaggio intelligibile dall'intelligenza artificiale, come evidenziato da F. Faggin, *Irriducibile: la coscienza, la vita, i computer e la nostra natura*, 2022, Milano, p. 300: «La conoscenza scientifica, che ha per oggetto solo il mondo esteriore conoscibile mediante relazioni matematiche e misurazione di eventi, è assolutamente necessaria, ma non basta per condurci alla conoscenza vissuta. Secondo me, l'obiettivo finale della conoscenza - a cui la scienza porta un contributo fondamentale - si realizza solo quando l'osservatore vive l'esperienza di se stesso e del mondo in modo integrale, perché la vera conoscenza va ben oltre l'aspetto simbolico della realtà».

sistema né permette di anticiparne deduttivamente le scelte decisionali. Ciò in quanto l'algoritmo ingloba e rielabora autonomamente le informazioni del data-set, e restituisce risultati non preventivabili a priori. Col che risulta quanto mai indispensabile porre massima attenzione alla configurazione e alla composizione del data-set, che deve essere neutrale, non discriminatorio, chiaro e trasparente.

Ecco perché la scelta del data-set è a tutti gli effetti un momento chiave nella progettazione del sistema d'intelligenza artificiale, e tale deve essere considerato anche per gli effetti legali conseguenti.

Come dire che la responsabilità dell'intelligenza artificiale deve essere necessariamente incanalata sul doppio binario dell'accertamento della responsabilità nelle fasi di programmazione dell'algoritmo e di configurazione del data-set, giacché l'intelligenza artificiale implementa un sistema deciso e costruito a monte dall'uomo, che, in un moderno *puppet-show*, è e deve rimanere responsabile per i risultati -anche non preventivabili in concreto- dei sistemi che lo stesso ha ideato e progettato.

L'ipotesi, peraltro diffusa in dottrina, di creare una nuova categoria giuridica, attribuendo una speciale forma di personalità all'intelligenza artificiale, si dimostra così del tutto inadeguata, siccome atta a deresponsabilizzare gli agenti umani tramite un'inverosimile fuga altrove.

In quest'ottica, risulta estremamente puntuale l'intervento europeo, che non si limita all'EU Artificial Intelligence Act, ma ha approntato un sistema regolatorio che coinvolge (o quanto meno tenta di coinvolgere) il complesso delle relazioni umane e digitali che afferiscono e partecipano al funzionamento dei sistemi d'intelligenza artificiale.

A tal proposito, l'EU Artificial Intelligence Act valuta i sistemi d'intelligenza artificiale in base al pericolo che gli stessi possono causare alla società in generale e alla tutela dei diritti fondamentali in particolare, imponendo obblighi di trasparenza crescenti in rapporto di diretta proporzionalità rispetto all'incremento di rischio del singolo sistema d'intelligenza artificiale considerato. Ciò parrebbe suggerire una valutazione in capo al legislatore europeo di intrinseca pericolosità dell'intelligenza artificiale, che tuttavia risulta stemperata dall'adozione degli altri strumenti regolatori di recente introduzione europea, ovverosia Data Act, Data Governance Act, Digital Services Act e Digital Markets Act[56].

Con questi quattro regolamenti, l'Unione, mentre introduce regole uniformi per l'accesso e l'utilizzo dei dati, facilitandone lo scambio e la condivisione tra settori e Stati membri, eleva la tutela digitale, all'uopo introducendo nuovi controllori specifici per il settore[57]. Ciò permette di ricondurre la governance dell'intelligenza artificiale ad un livello superiore, sovranazionale, prescindendo dalla localizzazione territoriale del singolo programmatore e degli utenti finali.

È dunque evidente che la direzione europea è sempre più tesa a instaurare un quadro sicuro per la condivisione dei dati all'interno dell'Unione, sul presupposto (come sopra postulato) che l'intelligenza artificiale possa operare in termini di legalità e affidabilità solo se fondata su un pacchetto sicuro, trasparente e affidabile di dati.

---

[56] Per Data Act si intende usualmente il Regolamento (UE) 2023/2854; il Regolamento (UE) 2022/868 è comunemente indicato come Data Governance Act, mentre il Digital Services Act è il Regolamento UE 2022/2065 e il Digital Markets Act è il Regolamento UE 2022/1925. A tali regolamenti si affianca, infine, la proposta di Direttiva europea sulla responsabilità dell'IA, COM(2022) 496 final, 28.9.2022, tuttora in discussione, su cui si rinvia a L.M. Lucarelli Tonini, *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova 327 proposta di "AI Liability Directive"*, in *Il Diritto Dell'informazione E Dell'informatica*, 2023, 2, p. 327 ss.

[57] In tale contesto, tramite l'art. 56 del DSA la Commissione europea avoca a sé poteri esclusivi di vigilanza contro possibili infrazioni e violazioni digitali, ed esercita tali poteri di concerto con le Autorità nazionali competenti ed in particolar modo con il Garante privacy del paese di stabilimento del sistema di IA interessato.

Nell'attuale contesto, in cui tanto si discute di intelligenza artificiale, soppesandone pro e contro, definendola trasparente o opaca, si corre il pericolo di trascurare l'importanza assoluta e centrale dei dati digitali. I dati rappresentano il fulcro, il motore e il propellente di qualunque sistema di intelligenza artificiale, e vanno dunque regolamentati non solo perché veicolano informazioni personali e sensibili, ma anche e soprattutto perché costituiscono la materia prima per il funzionamento dell'intelligenza artificiale.
Pare, invece, che mentre la dottrina europea si interroga sull'efficacia dell'EU Artificial Intelligence Act, risulta parzialmente adombrata la portata rivoluzionaria dei regolamenti europei sui dati, che determinano un allargamento esponenziale nei dati disponibili che, se non adeguatamente monitorato e controllato, potrebbe seriamente compromettere la sicurezza e la trasparenza reali dei sistemi d'intelligenza artificiale.
Dal combinato disposto delle regolamentazioni europee in materia di intelligenza artificiale e di dati digitali, emerge la necessità di rimodulare il settore della responsabilità civile per i danni prodotti dalle nuove tecnologie, senza tuttavia aprire a riconoscimenti di nuove categorie soggettive, ed in particolare senza prevedere nuove forme di personalità in capo a software, robot o sistemi artificiali, che non farebbe altro, in ultima analisi, che diminuire la tutela degli utenti finali.
Allo scopo, dunque, di ancorare sempre e comunque la tutela degli utenti finali, fruitori dei sistemi di intelligenza artificiale, ad un soggetto concretamente individuabile, cui ci si possa rivalere per eventuali azioni risarcitorie, a parere di chi scrive occorre escludere la possibilità di concepire una personalità giuridica artificiale e, parallelamente, va pure esclusa la configurabilità di una proprietà intellettuale artificiale.

INNOVAZIONE E TRADIZIONE: REGTECH, BLOCKCHAIN E INDICAZIONI GEOGRAFICHE

Riccardo Jovine[*]

SOMMARIO:
I. REGULATORY TECHNOLOGY: TRA INNOVAZIONE E CONFORMITÀ NORMATIVA; II. BLOCKCHAIN: DIFFERENZE E SVILUPPI TRA OCCIDENTE E ORIENTE; III. LE INDICAZIONI GEOGRAFICHE NELL'ECOSISTEMA BLOCKCHAIN: PROVA DELL'ORIGINE, COMPLIANCE E LOTTA ALLA CONTRAFFAZIONE; IV. PROMOZIONE DELLA SOSTENIBILITÀ ATTRAVERSO LA BLOCKCHAIN E LE INDICAZIONI GEOGRAFICHE; V. BLOCKCHAIN E INDICAZIONI GEOGRAFICHE: SFIDE E OPPORTUNITÀ.

L'intersezione tra innovazione tecnologica e tutela delle tradizioni, attraverso l'applicazione della Regulatory Technology (RegTech) e della blockchain nel settore delle indicazioni geografiche, prospetta nuove sfide ed opportunità. Attraverso una comparazione dello sviluppo e dell'implementazione di tali tecnologie nei diversi sistemi giuridici, come quelli europeo, statunitense e cinese, viene approfondito l'impatto giuridico e il ruolo che strumenti innovativi quali la blockchain e gli smart contracts possono rivestire nel settore alimentare, in particolare per la salvaguardia dei pilastri di provenienza, autenticità e qualità. Tali tecnologie contribuiscono a rafforzare la fiducia dei consumatori nei sistemi di certificazione, promuovendo al contempo la sostenibilità. Tuttavia, la piena realizzazione del loro potenziale richiede un elevato grado di consapevolezza del cambiamento tecnologico da parte del consumatore e un coinvolgimento attivo delle autorità pubbliche e private, le quali giocano un ruolo chiave in questo processo di trasformazione e protezione delle tradizioni.

The intersection between technological innovation and the protection of traditions, through the application of Regulatory Technology (RegTech) and blockchain in the field of geographical indications, presents new challenges and opportunities. By comparing the development and implementation of such technologies across different legal systems, such as those in Europe, the United States, and China, this study delves into the legal impact and the role that innovative tools like blockchain and smart contracts can play in the food sector, particularly for safeguarding the pillars of origin, authenticity, and quality. These technologies help to strengthen consumer trust in certification systems while promoting sustainability. However, the full realization of their potential requires a high level of consumer awareness regarding technological change and active involvement from both public and private authorities, who play a crucial role in this transformation process and the protection of traditions.

Keywords: RegTech – Blockchain – Indicazioni Geografiche – Provenienza – Autenticità – Qualità – Compliance normativa – Smart Contracts – Contraffazione – Sostenibilità – Tracciabilità – Sistemi giuridici comparati

[*] Riccardo Jovine is a PhD Candidate in Comparative Law and New Technologies Law at the European University of Rome, an Adjunct Professor of International Business Negotiation at Lorenzo de Medici Institute of Florence, and the Chief Operating Officer of the Italian Academy of the Internet Code. Formerly Riccardo was an Advisor for the Master's program in Food Law and Business at Luiss Guido Carli University, a Fellow of the Innovation Law Laboratory at the European University of Rome, a Fellow of the Law Journal Diritto Mercato Tecnologia (DIMT), a Fellow of the Sports Law Review at the Italian National Olympic Committee, a Research Scientist at Dorna WorldSBK, and a Research Fellow at Mercy University in New York. He is a member of research networks including the Italian Association of Comparative Law, the Interna-tional Institute of Communications (IIC), and the IP & Innovation Researchers of Asia Network (IPIRA). Riccardo Iovine. ORCID iD: 0009-0009-1302-4873. Email: riccardo.jovine@unier.it

I. REGULATORY TECHNOLOGY: TRA INNOVAZIONE E CONFORMITÀ NORMATIVA

L'applicazione delle tecnologie emergenti per migliorare la *compliance* normativa, meglio conosciuta come "Regulatory Technology" o "RegTech", prefigura importanti sviluppi nel campo del diritto e dell'innovazione.

Le origini della RegTech possono essere ricondotte alla crisi finanziaria del 2008, un periodo caratterizzato da notevoli turbolenze finanziarie e dalla successiva introduzione di misure normative più rigorose. Tuttavia, nonostante la RegTech venga spesso considerata solo nell'ambito dei servizi finanziari, le sue risorse applicative sono decisamente più ampie con un potenziale di innovazione significativo.[1]

Banche e organi regolatori devono affrontare sfide significative con alti costi operativi. I requisiti normativi, in particolare per le segnalazioni relative alle transazioni, aumentano il carico sulle banche, portando a una diminuzione della redditività in alcuni settori bancari. Negli ultimi dieci anni, infatti, la frequenza delle modifiche normative nel settore finanziario è aumentata notevolmente, con il succedersi di numerosi aggiornamenti regolamentari. Questo flusso di cambiamenti normativi è stato accompagnato da un aumento sia della frequenza che della gravità delle sanzioni in caso di *non compliance* con le normative di riferimento.[2]

Questo complesso panorama normativo ha dato origine alla Regulatory Technology come un approccio emergente focalizzato sull'utilizzo della tecnologia per aiutare le organizzazioni a conformarsi alle normative nei più svariati settori.

Nel settore sanitario, ad esempio, la RegTech può essere utilizzata per la gestione della

---

[1] J. BARBERIS, D. W. ARNER, R. P. BUCKLEY, *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*, Wiley (1st ed.), Chichester, 2019, i quali sottolineano come lo scambio reciproco degli approcci regolatori nei settori dei servizi finanziari e non finanziari possa stimolare l'innovazione. La RegTech affronta anche crimini finanziari, cybersecurity e protezione dei dati, rendendola rilevante in molteplici settori. Trova applicazione in aree come la cybersecurity, la privacy e persino in potenziali strumenti di informatica forense e software di e-discovery. Inoltre, la domanda di RegTech è portata avanti quale alternativa agli alti costi per la *compliance* normativa in vari settori. Ad esempio, i commercianti statunitensi spendono oltre 19.500 dollari per dipendente all'anno in costi legati alla *compliance* normativa. Comprendere questi costi può aiutare a individuare le aree in cui la RegTech potrebbe essere più vantaggiosa, includendo sia i costi di conformità che i costi di rimedio in caso di violazioni regolatorie.

[2] Durante la prima metà del 2023, i regolatori finanziari internazionali hanno imposto un totale combinato di 97 multe, per un totale di 189 milioni di dollari, per non conformità con le normative anti-riciclaggio (AML), inclusi Know Your Customer (KYC) e Client Due Diligence (CDD), oltre a violazioni delle sanzioni. Queste multe sono state imposte per far rispettare la conformità e scoraggiare le violazioni relative ai crimini finanziari. Il numero di multe imposte nella seconda metà del 2023 ha già superato questo conteggio. Nel primo semestre del 2022, gli organismi di regolamentazione hanno accumulato multe per un totale di 1,5 miliardi di dollari per violazioni che si estendono tra EMEA, Nord America e Asia. Tradizionalmente, la seconda metà degli anni solari ha visto un aumento delle azioni esecutive. Tuttavia, i risultati convalidano un andamento pluriennale di diminuzione delle multe, raggiungendo il picco nel 2020 con oltre 10 miliardi di dollari. Dati disponibili su: https://member.regtechanalyst.com/. Ad esempio, nella prima metà del 2023, Wells Fargo ha ricevuto la multa collettiva più grande, pari a 97,8 milioni di dollari, imposta dalla Federal Reserve degli Stati Uniti e dal Dipartimento del Tesoro per aver permesso a una banca estera non identificata di effettuare centinaia di milioni di dollari in transazioni sulla sua piattaforma finanziaria Eximbills, nonostante fosse proibito farlo a causa delle sanzioni statunitensi contro Iran, Siria e Sudan. Inoltre, il settore delle criptovalute ha affrontato multe significative, con casi rilevanti come Binance, multata per quasi 5 miliardi di dollari per violazione delle leggi statunitensi anti-riciclaggio di denaro. Binance è stata accusata di violare il Bank Secrecy Act permettendo ai clienti di commerciare senza adeguati controlli KYC. Questa lacuna nei controlli di conformità ha permesso transazioni con individui sanzionati e reti criminali, collegando la piattaforma ad attività illegali come traffico di droga e tratta di esseri umani. Ulteriori aggiornamenti disponibili su: https://www.forbes.com e https://www.nytimes.com.

conformità normativa, in particolare con riferimento a regolamenti come l'Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti. Ciò include la protezione della privacy dei dati dei pazienti, la gestione delle cartelle cliniche elettroniche e la garanzia di una condivisione sicura dei dati tra le istituzioni.

Le soluzioni avanzate della RegTech sono anche in grado di utilizzare l'intelligenza artificiale per automatizzare i controlli di conformità e mantenere aggiornati i registri del consenso dei pazienti, dell'accesso ai dati e delle attività di trattamento dei dati.[3]

Inoltre, la RegTech potrebbe svolgere un ruolo significativo nell'assicurare che le aziende rispettino le leggi sulla protezione dei dati, come ad esempio il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea, o GDPR. Un sistema RegTech potrebbe automatizzare la mappatura e la classificazione dei dati personali nei sistemi di un'organizzazione, assistere nel monitoraggio in tempo reale delle violazioni dei dati e supportare la gestione delle richieste di accesso agli stessi.[4]

Nel settore alimentare, la RegTech prefigura applicazioni di rilievo in grado di garantire la conformità alle normative e agli standard di sicurezza alimentare, fornendo, tramite la tecnologia, una registrazione trasparente e verificabile dell'intera *supply chain*, a partire dall'origine e proseguendo nelle diverse fasi di lavorazione e distribuzione dei prodotti alimentari.[5]

II. BLOCKCHAIN: DIFFERENZE E SVILUPPI TRA OCCIDENTE E ORIENTE

In questo contesto, il coinvolgimento del settore pubblico riveste un ruolo chiave nell'ecosistema della RegTech. Le autorità governative potrebbero infatti adottare la

[3] Sul punto, si veda: J. BARBERIS, D. W. ARNER, R. P. BUCKLEY, *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*, cit., che sottolineano come un fornitore di servizi sanitari o assicuratore potrebbe dover monitorare la doppia conformità con l'Health Insurance Portability and Accountability Act statunitense e il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea per mantenere gli stessi record dei pazienti.

[4] Vedi: P. RYAN, M. CRANE, R. BRENNAN, *Design Challenges for GDPR RegTech*, in *Proceedings of the 22nd International Conference on Enterprise Information Systems*, 2020, in cui gli autori esaminano l'efficacia della RegTech nel migliorare la conformità al GDPR, con particolare attenzione al Principio di Responsabilità. I risultati suggeriscono che un approccio RegTech non solo offre una conformità più robusta e verificabile con il GDPR, ma porta anche con sé i vantaggi intrinseci di riduzione dei rischi e risparmi sui costi. Implementare una strategia RegTech per la conformità al GDPR può quindi aiutare efficacemente un'organizzazione a soddisfare i propri obblighi di responsabilità, dimostrando il potenziale della RegTech di trasformare i processi di *compliance* al GDPR.

[5] In letteratura, si veda: A. STAZI, R. JOVINE, *GMOs, Food Traceability and RegTech: Genetically Modified Food, Traceability Systems and Blockchain as a Regulatory Technology*, Springer, Switzerland, 2024, pp. 129 ff., in cui gli autori evidenziano come la Regulatory Technology, attraverso tecnologie emergenti basate su registri distribuiti come la blockchain, prefigura nuovi modelli organizzativi e normativi per una gestione più efficace dei sistemi di tracciabilità all'interno della filiera alimentare. La RegTech, mediante tecnologie come la blockchain, può essere applicata anche agli alimenti geneticamente modificati, apportando significativi vantaggi sia strutturali che sostanziali.

J. LI, A. MAITI, J. FEI, *Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things*, in *Future Internet*, 2023, Vol. 15, No. 8, in cui gli autori sottolineano come il settore agricolo affronti numerose sfide legate alla *compliance* normativa, tra cui le normative ambientali, le normative sulla sicurezza alimentare e i requisiti di trasparenza della filiera. Le soluzioni RegTech possono aiutare le aziende a conformarsi a queste normative e migliorare le loro operazioni complessive. Ad esempio, la RegTech può monitorare la conformità alle normative sulla sicurezza alimentare, tracciare l'uso di pesticidi e altri prodotti chimici, garantire che gli agricoltori rispettino gli standard ambientali, migliorare la tracciabilità e la trasparenza nella filiera e potenziare la gestione del rischio.

tecnologia per ottimizzare le loro funzioni regolamentari, risparmiando risorse e migliorando l'efficienza.

L'Unione Europea, ad esempio, sta compiendo un grande sforzo per dare forma a un quadro normativo sulle tecnologie blockchain. In questo senso, sono state promosse diverse iniziative da parte della Commissione Europea volte ad approfondire il fenomeno, in particolare nel settore alimentare.[6]

Nel febbraio 2023, la Commissione Europea ha reso operativo il *Sandbox* regolamentare pan-europeo sulla blockchain,[7] precedentemente annunciato,[8] con l'obiettivo di raggiungere, tramite le migliori pratiche nel campo delle *Distributed Ledger Technologies* (DLT), uno sviluppo normativo relativo alla conformità normativa.

Il *Sandbox* sarà operativo fino al 2026, offrendo un'opportunità di dialogo tra diversi attori con la presenza centrale delle autorità di regolamentazione nazionali, al fine di garantire certezza giuridica e rispetto del principio di neutralità tecnologica.[9]

L'impegno dell'Unione Europea verso la tecnologia blockchain e la RegTech è altresì riscontrabile nelle più recenti misure. Il Regolamento sui Mercati delle Cripto-Attività n. 2023/1114 (Regolamento MiCA) rappresenta un esempio di questo impegno volto ad affrontare la frammentazione del quadro giuridico applicabile alle cripto-attività.[10]

Anche negli Stati Uniti, molti Stati hanno adottato misure legislative volte a regolamentare le tecnologie blockchain in considerazione della loro natura innovativa e soprattutto delle

---

[6] S. NASCIMENTO, A. PÓLVORA, J. S. LOURENÇO, *#Blockchain4EU: Blockchain for Industrial Transformations (EUR 29215 EN)*, in *JRC Publications Repository*, 2018, in cui si evidenzia l'utile applicazione delle tecnologie blockchain nell'industria alimentare; Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: costruire fiducia con la disintermediazione (2017/2772(RSP)), in cui viene attribuita rilevanza alla tecnologia blockchain come strumento che "può democratizzare i dati e migliorare la fiducia e la trasparenza"; Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni "Il Futuro dell'Alimentazione e dell'Agricoltura" COM(2017) 713 final, 13-15.

[7] Un sandbox è un sistema che riunisce regolatori, aziende ed esperti tecnologici per testare soluzioni innovative e identificare gli ostacoli che sorgono nel loro dispiegamento.

[8] Conclusioni del Consiglio sugli spazi di sperimentazione normativa e sulle clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, resiliente e a prova di futuro, in grado di affrontare le sfide dirompenti dell'era digitale 2020/C 447/01, disponibile all'indirizzo: https://eur-lex.europa.eu/.

[9] Maggiori informazioni sul Sandbox Blockchain Europeo sono disponibili all'indirizzo: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project.

[10] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (ELI: 01-09). Il Regolamento si applica agli emittenti e agli offerenti di cripto-attività e ai fornitori di servizi relativi alle cripto-attività. Tra i principali obblighi, l'Articolo 1 prevede: "a) gli obblighi di trasparenza e informativa per l'emissione, l'offerta al pubblico e l'ammissione di cripto-attività alla negoziazione su una piattaforma di negoziazione per cripto-attività («ammissione alla negoziazione»); b) i requisiti per l'autorizzazione e la vigilanza dei prestatori di servizi per le cripto-attività, degli emittenti di token collegati ad attività e degli emittenti di token di moneta elettronica, nonché per il loro funzionamento, la loro organizzazione e la loro governance; c) i requisiti per la tutela dei possessori di cripto-attività nell'emissione, nell'offerta al pubblico e nell'ammissione alla negoziazione di cripto-attività; d) i requisiti per la tutela dei clienti di prestatori di servizi per le cripto-attività; e) le misure volte a prevenire l'abuso di informazioni privilegiate, la comunicazione illecita di informazioni privilegiate e la manipolazione del mercato in relazione alle cripto-attività, al fine di garantire l'integrità dei mercati delle cripto-attività." Il testo ufficiale è disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114.

loro molteplici applicazioni nel settore commerciale, tra cui quello alimentare.[11]
Spostando l'attenzione al mondo asiatico e in particolare al sistema cinese, nel gennaio 2019 l'Amministrazione del Cyberspazio ha presentato le prime Disposizioni Amministrative sulla Blockchain, stabilendo il contenuto di base e le regole di registrazione per le entità che offrono funzionalità blockchain come servizio e prevedendo multe e altre sanzioni per le possibili violazioni. [12]
Tuttavia, nel settembre 2021, la Banca Popolare Cinese e altre nove autorità, tra cui le principali istituzioni legali e finanziarie, hanno emesso una direttiva volta a frenare i rischi speculativi associati al trading di criptovalute.[13] Questa mossa ha rafforzato l'impostazione secondo cui le criptovalute come Bitcoin non possiedono lo stesso status legale delle valute fiat, ribadendo i principi enunciati in una analoga circolare del 2017.[14]
Il rigido approccio della Cina contro le criptovalute ha spesso oscurato il forte impegno del Paese nello sviluppo delle tecnologie blockchain.
Le recenti "Opinioni Guida dei Due Ministeri sull'Accelerazione della Promozione dell'Applicazione della Tecnologia Blockchain e dello Sviluppo Industriale", rilasciate congiuntamente dal Ministero dell'Industria e della Tecnologia dell'Informazione e dall'Agenzia per la Sicurezza Cibernetica, illustrano la determinazione della Repubblica Popolare Cinese a perseguire lo sviluppo delle tecnologie blockchain come supporto del

[11] Ai sensi delle Federal Rules of Evidence, in particolare la Regola 1002, è stabilito che è necessario un originale scritto, registrato o fotografico per provare il suo contenuto, salvo che le regole federali o gli statuti prevedano diversamente. Sebbene il testo stabilisca uno standard minimo per le prove, non affronta specificamente l'uso della tecnologia blockchain. Diversi Stati hanno intrapreso azioni per affrontare questa questione, con New York pioniere nella regolamentazione delle criptovalute. Attualmente, 32 stati negli USA hanno implementato proprie norme e regolamenti riguardanti la blockchain. Tra le misure più rilevanti si veda il Senate Bill 5638 – 2019 – 2020 adottato dallo Stato di Washington, che oltre a fornire una definizione di tecnologie blockchain e registro distribuito, riconosce la validità della tecnologia a registro distribuito affermando che: "A un registro elettronico o una firma elettronica non possono essere negati gli effetti legali, validità o applicabilità solo perché generati, comunicati, ricevuti o archiviati utilizzando la tecnologia a registro distribuito". In questa direzione si muovono le regolamentazioni di altri Stati, disponibili all'indirizzo: https://www.ncsl.org. In letteratura, si veda: A. STAZI, *Smart Contracts and Comparative Law: A Western Perspective*, Springer Nature, Switzerland, 2021, pp. 91 e seguenti.
[12] Il "Regolamento sulla Gestione dei Servizi di Informazione Blockchain" deliberato e approvato dall'Ufficio Nazionale per l'Informazione su Internet, entrato in vigore il 15 febbraio 2019. Testo ufficiale disponibile all'indirizzo: http://www.cac.gov.cn/2019-01/10/c_1123971164.htm.
[13] Documento ufficiale disponibile all'indirizzo: https://perma.cc/DC7U-MSDF.
[14] Circolare disponibile all'indirizzo: https://perma.cc/N88N-5CV5. Tra i punti salienti della circolare del 2021 della PBOC: ribadisce che le criptovalute non sono riconosciute come moneta legale in Cina. Non sono emesse da alcuna autorità monetaria e, pertanto, non possono essere accettate sul mercato come valuta; si dichiara esplicitamente illegale ogni forma di transazione in criptovalute. Ciò include attività come la conversione di criptovalute, il trading, gli ICO e la fornitura di servizi finanziari correlati alle criptovalute. Il documento sottolinea che banche e istituzioni finanziarie hanno espresso divieto di facilitare qualsiasi transazione relativa alle criptovalute. Il raggio d'azione si estende agli scambi di criptovalute esteri che hanno come destinatari residenti cinesi. Affermando che sia i player di questi scambi in Cina che coloro che forniscono servizi a questi sarebbero soggetti a conseguenze legali se partecipano o facilitano transazioni in criptovalute; si delinea un approccio collaborativo tra le autorità per monitorare e reprimere severamente le attività illegali relative alle criptovalute, sia online che offline. Queste attività includono il riciclaggio di denaro e il gioco d'azzardo transfrontaliero, ma non sono limitate ad essi. Inoltre, gli investitori sono avvertiti sui rischi legali associati agli investimenti in criptovalute. La circolare osserva che qualsiasi azione legale civile relativa a tali investimenti che violano l'ordine pubblico e il buon costume sarebbe considerata invalida, con gli investitori che dovranno sopportare le relative perdite.

progresso industriale.[15]

Questa iniziativa rivela una differenziazione strategica tra l'approccio del Paese verso le criptovalute e la sua visione più ampia verso la tecnologia blockchain, riconoscendone il potenziale atto a favorire un significativo progresso.

In relazione al settore alimentare, le caratteristiche della blockchain appaiono utili alleati delle proprietà di provenienza, autenticità e qualità, pilastri dei prodotti ad indicazione geografica.

Tale utilità è rinvenibile sotto molteplici aspetti con particolare riferimento alla prova dell'origine e alla *compliance* ai disciplinari di riferimento, alla lotta alla contraffazione, e alla promozione della sostenibilità.

III. LE INDICAZIONI GEOGRAFICHE NELL'ECOSISTEMA BLOCKCHAIN: PROVA DELL'ORIGINE, COMPLIANCE E LOTTA ALLA CONTRAFFAZIONE

In merito ad una possibile registrazione su blockchain delle indicazioni geografiche, sebbene l'ecosistema blockchain comporti una sicurezza unica e incomparabile rispetto a qualsiasi altra forma di registrazione analogica o digitale, occorre rilevare che le peculiarità del sistema delle indicazioni geografiche rendono l'eventuale utilizzo della blockchain più complesso rispetto ad altri diritti di proprietà intellettuale, come ad esempio il diritto d'autore.[16]

Il primo aspetto di rilievo nell'utilizzo di un sistema blockchain è rappresentato dalla prova d'origine e dalla *compliance* ai disciplinari di riferimento.

Nell'Unione Europea il requisito principale per la protezione delle indicazioni geografiche è difatti garantire il rispetto degli standard IG.

Il sistema dell'Unione Europea si basa prevalentemente su autorità pubbliche riconosciute[17] volte ad assicurare la conformità alle specifiche delle Denominazioni di Origine Protetta e delle Indicazioni Geografiche Protette anche nell'ambito digitale.[18]

---

[15] "Opinioni Guida dei Dipartimenti sull'Accelerazione dell'Applicazione della Blockchain e dello Sviluppo Industriale" (**两部门关于加快推**动**区**块链**技**术应**用和**产业发**展的指**导**意**见) sono disponibili all'indirizzo:
https://www.miit.gov.cn/zwgk/zcwj/wjfb/rjy/art/2021/art_851f2059f13d41a8bba59c8dce9401a8.html.

[16] A tal proposito sono nati progetti come Tutelio o Creativitysafe. Per saperne di più su queste ed altre startup consultare i seguenti link: https://creativitysafe.com/; https://www.tutelio.org/; https://musicoin.org/; http://www.certo.legal/. In letteratura, si veda: R. JOVINE, *Blockchain e proprietà intellettuale: opportunità e questioni giuridiche*, in *Diritto Mercato Tecnologia (DIMT)*, 2020, in cui l'autore analizza, in chiave comparata, le possibili applicazioni della tecnologia blockchain al diritto d'autore.

[17] Regolamento (UE) 2024/1143, Articolo 39: "1. Ai fini del presente capo, ciascun operatore che intenda partecipare ad attività previste dal disciplinare di un prodotto designato da un'indicazione geografica ne dà notifica alle autorità competenti, agli organismi delegati o alle persone fisiche di cui al paragrafo 3, lettere a) e b). Gli Stati membri redigono e tengono aggiornato un elenco degli operatori che svolgono attività soggette a uno o più obblighi previsti dal disciplinare di un prodotto designato da un'indicazione geografica iscritta nel registro delle indicazioni geografiche dell'Unione originarie del loro territorio."

[18] Regolamento (UE) 2024/1143, Articolo 42, paragrafo 1 e 2: "1. Gli Stati membri designano una o più autorità competenti responsabili sia di verificare che di tutelare l'uso delle indicazioni geografiche dopo che il prodotto designato da un'indicazione geografica sia stato immesso sul mercato, il che comprende operazioni quali deposito, transito, distribuzione o offerta in vendita, anche nel settore del commercio elettronico. Tali autorità possono coincidere con le autorità competenti di cui all'articolo 39, paragrafo 3, lettera a), del presente regolamento e all'articolo 116 bis, paragrafo 2, del regolamento (UE) n. 1308/2013. 2. Le autorità di cui al paragrafo 1 si adoperano, periodicamente e con una frequenza adeguata sulla base dell'analisi del rischio e delle notifiche ricevute, anche dai gruppi di produttori, al fine di garantire il rispetto

Difatti, sebbene i produttori siano responsabili dei propri controlli interni volti a garantire la conformità al disciplinare [19] dei prodotti immessi sul mercato, la verifica di tali adempimenti è effettuata dalle autorità competenti dello Stato di appartenenza.
Negli Stati Uniti d'America, invece, la concezione privatistica del sistema di "common law" rispecchia anche la protezione degli standard geografici. Difatti il sistema delle indicazioni geografiche negli Stati Uniti si avvale delle strutture amministrative già esistenti per i marchi, consentendo a qualsiasi parte interessata di opporsi o di richiedere la cancellazione di un'indicazione geografica registrata qualora ritenga che la registrazione o la sua permanenza le arrechi danno.[20]
Rispetto alla prova dell'origine e alla *compliance* ai disciplinari di riferimento, in qualsiasi modo vengano trattate le indicazioni geografiche, sistema *sui generis*, dei marchi o misto come quello cinese, [21] l'applicazione della blockchain appare comunque possibile e

del disciplinare o del documento unico o di un equivalente di quest'ultimo per l'indicazione geografica in questione, anche nelle presentazioni online e nell'etichettatura."

[19] Regolamento (UE) 2024/1143, Articolo 49: "1. Un disciplinare comprende almeno gli elementi seguenti: a) il nome da registrare come denominazione di origine o indicazione geografica, quale usato nel commercio o nel linguaggio comune per descrivere il prodotto specifico nella zona geografica delimitata; b) la descrizione del prodotto, comprese se del caso le materie prime, le varietà vegetali e le razze animali interessate, nonché la denominazione commerciale della specie e il suo nome scientifico, oltre alle principali caratteristiche fisiche, chimiche, microbiologiche od organolettiche del prodotto; c) la definizione della zona geografica delimitata riguardo al legame di cui alla lettera f), punto i) o punto ii), del presente paragrafo e, se del caso, gli elementi che indicano il rispetto delle condizioni di cui all'articolo 46, paragrafo 3; d) gli elementi che dimostrano che il prodotto proviene dalla zona geografica delimitata specificata in conformità dell'articolo 46, paragrafo 1, lettera c), o dell'articolo 46, paragrafo 2, lettera c); e) la descrizione del metodo di ottenimento del prodotto e, se del caso, dei metodi di produzione locali, autentici e costanti; nonché informazioni relative al confezionamento, quando il gruppo di produttori richiedente stabilisce in tal senso e fornisce sufficienti motivazioni specifiche per prodotto per cui il confezionamento deve aver luogo nella zona geografica delimitata per salvaguardare la qualità, garantire l'origine o assicurare il controllo, tenendo conto del diritto dell'Unione, in particolare in materia di libera circolazione dei prodotti e libera prestazione di servizi; f) gli elementi che stabiliscono: i) per quanto riguarda una denominazione di origine protetta, il legame fra la qualità o le caratteristiche del prodotto e l'ambiente geografico di cui all'articolo 46, paragrafo 1, lettera b). I dettagli riguardanti i fattori umani dell'ambiente geografico possono, se del caso, limitarsi a una descrizione del suolo e della gestione del paesaggio, delle pratiche di coltivazione o di qualunque altro contributo umano volto al mantenimento dei fattori naturali dell'ambiente geografico di cui a tale disposizione; ii) per quanto riguarda un'indicazione geografica protetta, il legame fra una data qualità, la reputazione o un'altra caratteristica del prodotto e l'origine geografica di cui all'articolo 46, paragrafo 2, lettera b). 2.Il disciplinare può includere anche: a) le pratiche sostenibili di cui all'articolo 7; b) qualsiasi regola specifica per l'etichettatura del prodotto in questione; c) altre condizioni applicabili ove previsto dallo Stato membro o da un gruppo di produttori, se del caso, tenendo conto del fatto che tali condizioni devono essere oggettive, non discriminatorie e compatibili con il diritto dell'Unione e nazionale."

[20] 15 U.S. Code § 1064 - Cancellation of registration: "A petition to cancel a registration of a mark, stating the grounds relied upon, may, upon payment of the prescribed fee, be filed as follows by any person who believes that he is or will be damaged, including as a result of a likelihood of dilution by blurring or dilution by tarnishment under section 1125(c) of this title, by the registration of a mark on the principal register established by this chapter, or under the Act of March 3, 1881, or the Act of February 20, 1905: (1)Within five years from the date of the registration of the mark under this chapter. (2)Within five years from the date of publication under section 1062(c) of this title of a mark registered under the Act of March 3, 1881, or the Act of February 20, 1905."

[21] In letteratura, si veda: A. STAZI, R. JOVINE, *GMOs, Food Traceability and RegTech: Genetically Modified Food, Traceability Systems and Blockchain as a Regulatory Technology*, cit., in cui gli autori evidenziano come da un punto di vista comparato, l'Unione Europea si distingue per il suo sistema *sui generis*, basato sui concetti di *terroir* e reputazione, che non solo incrementa il valore di mercato, ma preserva anche il patrimonio culturale proteggendo i prodotti alimentari regionali; gli Stati Uniti adottano un approccio incentrato sui marchi, che privilegia la protezione del marchio e del nome, ponendo meno enfasi sulla specificità regionale; e la Cina

vantaggiosa, sia da un punto di vista strutturale che sostanziale.[22]

Dal punto di vista strutturale,[23] i principali vantaggi derivanti dall'utilizzo di un registro blockchain sono rappresentati da: i) decentralizzazione, che determina la transnazionalità delle informazioni contenute; ii) immutabilità, da intendersi come modalità non distruttiva di registrare e tracciare le informazioni affinchè ogni cambiamento non cancelli il precedente ma ne rappresenti uno nuovo; iii) crittografia, che garantisce la sicurezza delle informazioni e l'inalterabilità dei dati; iv) trasparenza, dovuta alla completa accessibilità da parte di tutte o di alcune parti autorizzate a seconda della forma di governance prescelta.[24]

Da un punto di vista sostanziale, i benefici derivanti dall'utilizzo della blockchain sono molteplici.

Immaginando una *supply chain* alimentare digitale e condivisa con la blockchain sarebbe possibile tracciare qualsiasi prodotto in ogni fase: produzione, lavorazione, trasporto, stoccaggio, distribuzione e vendita, coinvolgendo tutte le parti interessate.

Ciò consentirebbe alle parti interessate di avvalersi di un registro "interoperabile"[25] e trasparente in un contesto collaborativo nonché in *compliance* con la normativa vigente.[26]

Inoltre le indicazioni geografiche, inserite nel registro blockchain dell'intera supply chain, potrebbero essere a disposizione dei competenti organismi di controllo nonché del

sta rafforzando il proprio regime di protezione delle IG, con l'obiettivo di promuovere il patrimonio agricolo e accrescere la propria presenza sul mercato.

[22] Tra i progetti di maggiore rilievo si annovera l'IBM Food Trust, basato sulla tecnologia Hyperledger e frutto di una collaborazione tra importanti attori e istituzioni quali IBM, Walmart, JD.com e l'Università Tsinghua in Cina. La soluzione consente agli utenti autorizzati di accedere immediatamente a dati operativi della filiera alimentare, dal produttore al punto vendita, fino al consumatore finale. La cronologia completa e l'ubicazione attuale di ciascun prodotto alimentare, unitamente ad informazioni aggiuntive quali certificazioni, dati di test e dati relativi alla temperatura, sono disponibili in pochi secondi non appena caricati sulla blockchain. (https://www.ibm.com/blockchain/solutions/food-trust).

[23] A tal proposito, si veda: P. FILIPPI, A. WRIGHT, *Blockchain and the law: the Rule of Code*, cit., pp. 33-57; G. SLAVIOTTI, L. M. DE ROSSI, N. ABBATEMARCO, *The Blockchain Journey*, cit., pp. 8 e seguenti, che analizzano le caratteristiche peculiari dei sistemi blockchain.

[24] In letteratura, si veda: G. SLAVIOTTI, L. M. DE ROSSI, N. ABBATEMARCO, *The Blockchain Journey,*, cit., pp. 23 e seguenti, i quali sottolineano che un modello di governance basato sulla blockchain può essere classificato principalmente in due dimensioni: "permissioned/permissionless" e "public/private". "La prima si riferisce alla capacità di partecipare al meccanismo di consenso, mentre la seconda è legata alla possibilità per un utente di accedere all'applicazione blockchain. In un ecosistema pubblico, chiunque può unirsi alla rete e utilizzare l'applicazione anche senza l'autorizzazione del fornitore di servizi. Non c'è un'autorità centrale e chiunque con una connessione Internet può utilizzare il servizio, leggere la cronologia delle transazioni e, eventualmente, partecipare al meccanismo di consenso. In una blockchain privata, gli utenti finali sono conosciuti e verificati, e saranno in grado di accedere al servizio blockchain solo se il fornitore di servizi lo consente." Si veda anche: A. STAZI, *Smart Contracts and Comparative Law: A Western Perspective*, cit., pp. 73-74.

[25] Da intendersi quale interoperabilità interna, poiché l'interoperabilità cross-chain rappresenta ancora una delle questioni critiche che ostacolano l'adozione diffusa delle applicazioni blockchain. A tal proposito, si veda: M. MADINE, K. SALAH, R. JAYARAMAN, Y. AL-HAMMADI, *AppXchain: Application-Level Interoperability for Blockchain Networks*, in *IEEE*, 2021, Vol 99, pp. 87777 – 87789.

[26] Le norme conformi alla legislazione di uno specifico Stato, nonché le regole operative del registro, possono essere stabilite tramite contratti intelligenti, "protocolli informatici che si eseguono autonomamente applicando stringhe di codice per cui sono stati programmati." Si veda: A. STAZI, *Smart Contracts and Comparative Law: A Western Perspective*, cit., pp. 75 ss. Sullo sviluppo dei contratti intelligenti nel settore alimentare, si veda: J. FRANK, *Blockchain Functionality: How Smart Contracts Can Save Small Farms*, in *New York Law School Law Review*, 2020, pp. 17 e seguenti, dove si sottolinea come i contratti intelligenti possano orchestrare la vendita di beni, gestire la logistica della catena di approvvigionamento e controllare il passaggio di proprietà di beni immobili, offrendo in particolare ai piccoli agricoltori un'opportunità preziosa per essere competitivi in un'industria agricola dinamica.

pubblico dei consumatori per aumentarne la consapevolezza informativa.[27]
Si prenda ad esempio il prodotto Speck Alto Adige IGP ("Südtiroler Markenspeck" o "Südtiroler Speck") il cui disciplinare prevede che: (i) la zona di produzione consista nel territorio della Provincia Autonoma di Bolzano – Alto Adige (Südtirol); (ii) la materia prima consista in cosce di suino disossate, rifilate con o senza fesa; (iii) il metodo di elaborazione consista nel salare e aromatizzare la coscia di suino disossata, affumicata "a freddo" in locali appositi, ad una temperatura massima di 20°C e ben stagionata secondo gli usi e le tradizioni locali.[28]
Con riferimento all'esempio citato, i produttori dello Speck Alto Adige IGP potrebbero inserire le relative informazioni sulla blockchain per integrare e supportare gli standard di certificazione: la materia prima consistente in cosce di suino, il metodo di elaborazione, la temperatura, il lotto e così via.
Ogni informazione verrebbe così notarizzata nel sistema andando a creare per ogni prodotto un'impronta digitale che ne certifica l'esistenza fisica e digitale seguita dalla documentazione relativa alle caratteristiche del prodotto ad indicazione geografica.
In tal modo gli organi di controllo potrebbero avere accesso ad un unico sistema blockchain per una valutazione della conformità risparmiando tempo e sforzi per adattarsi alle metodologie utilizzate da ogni produttore.[29]
La validazione della conformità agli standard potrebbe avvenire mediante l'applicazione di *smart contract*[30] al fine di impedire che prodotti non conformi raggiungano il mercato. Per illustrare come uno *smart contract* sarebbe vantaggioso per le indicazioni geografiche, possiamo prendere ad esempio il trasferimento di un lotto di una "Mozzarella di Bufala Campana DOP" dal produttore ad uno stabilimento di confezionamento.

---

[27] In letteratura, si veda: A. STAZI, R. JOVINE, *Food Traceability in Europe, the US and China: A Comparative and Technological Analysis*, in *BioLaw Journal*, 2022, Vol. 2, pp. 399-425, in cui gli autori analizzano il tema della tracciabilità alimentare basato su un sistema blockchain individuando pro e contro del sistema di riferimento, analizzando altresì le normative in materia in prospettiva comparata.
[28] Disciplinare presente su:
https://www.politicheagricole.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/3339
[29] In letteratura, si veda: S. M. ARONZON, *Blockchain and geographical indications: a natural fit?*, in *Journal of Intellectual Property Law & Practice*, 2020, p. 5; e M. S. CADOGAN, *The Prospects and Limits of Blockchain Technologies in the Global Protection of Geographical Indications*, in *Intellectual Property Institute of Canada*, 2020, Vol. 35, p. 32
[30] Se un contratto tradizionale è formulato per essere compreso e interpretato dagli esseri umani, lo *smart contract* è redatto affinché possa essere interpretato ed eseguito dal software all'interno della blockchain. La logica che governa la redazione di uno *smart contract* è basata sul principio "if this then that", indicando che al verificarsi di certe condizioni specificate, seguiranno determinati effetti. Affinché l'esecuzione degli *smart contracts* sia efficace, è essenziale che siano collegati a valori di scambio o a fonti esterne denominate "oracles". Questo collegamento rende possibile l'esecuzione automatica del contratto, prevenendo qualsiasi forma di inadempimento. La programmazione degli *smart contracts* può includere funzioni interne come il "self-destruct" o il "call", che permettono modifiche nello stato del contratto mantenendo l'immutabilità della tracciabilità all'interno della blockchain. È fondamentale distinguere tra gli smart code contracts, che non contengono elementi legali ma seguono la funzione classica degli smart contracts tramite oracoli che definiscono le condizioni per la loro esecuzione, e gli smart legal contracts, che includono specifici contenuti legali. La distinzione è rilevante poiché, se non redatti o eseguiti correttamente, gli smart legal contracts possono incorrere in violazioni legali. Questi ultimi rappresentano un tipo di contratto negoziale eseguito tramite codice informatico, la cui valutazione legale dipenderà dalla legislazione applicabile al contratto sottostante. In letteratura, si veda: A. STAZI, *Smart Contracts and Comparative Law: A Western Perspective*, cit.; A. STAZI, *Smart Contracts: Elements, Pathologies and Remedies*, forthcoming in Loo J, Leon NR (eds), Law and Change: An Asian Perspective, 2024; A. M. GAMBINO, A. STAZI, *Contract automation from telematic agreements to smart contracts*, in *The Italian Law Journal*, 2021, Vol 7, No. 1, pp. 97–115.

Gli standard che il formaggio fresco deve rispettare per la protezione IG sono: (i) prodotto con latte di bufala intero fresco; (ii) gli allevamenti bufalini devono essere di razza mediterranea; (iii) la coagulazione, previo riscaldamento del latte, deve avvenire ad una temperatura tra i 33°C e i 39°C.

Il produttore, mediante una combinazione di input umani e sensori elettronici, potrebbe inserire nella blockchain tutte le informazioni relative alla specifica indicazione geografica: quale tipo di latte è stato utilizzato, da quali animali è stato ottenuto il latte, come sono stati allevati gli animali, la temperatura a cui il formaggio fresco dev'essere conservato, etc. Successivamente, il produttore trasporterebbe fisicamente il prodotto allo stabilimento di confezionamento.

Uno *smart contract* può essere registrato nell'ecosistema blockchain per trovare attivazione in ricezione agli input del produttore. Nell'esempio citato, se gli input confermano che il formaggio fresco è in *compliance* con il disciplinare, allora uno *smart contract* eseguirà automaticamente la registrazione nella blockchain evidenziando che il lotto è conforme agli standard al momento della ricezione da parte dello stabilimento.

L'uso di uno *smart contract* per validare la conformità sarebbe già vantaggioso di per sé, ma si potrebbe anche immaginare di andare oltre, utilizzando lo *smart contract* per impedire che prodotti non conformi arrivino sul mercato.

Si potrebbe mettere in atto un processo per cui, una volta che il successivo operatore di riferimento riceve il prodotto, ne registra la ricezione fisica nella blockchain. Poi, non appena la blockchain contiene la conferma della ricezione, l'output dello *smart contract* valida la conformità del lotto. La catena di approvvigionamento virtuale del prodotto potrebbe poi procedere mediante altri *smart contract* successivi.

Se uno degli input iniziali del produttore però non è conforme, ad esempio nel caso in cui il prodotto non è stato conservato alla temperatura desiderata, lo *smart contract* non avrà esecuzione. Di conseguenza il lotto del prodotto non conforme non potrebbe raggiungere il mercato.

In merito alle pratiche di contraffazione dei prodotti alimentari, l'ecosistema blockchain, vista la sua caratteristica della immutabilità, renderebbe tali pratiche facilmente individuabili da parte delle autorità di controllo.[31]

[31] In letteratura, si veda: M. S. CADOGAN, *The Prospects and Limits of Blockchain Technologies in the Global Protection of Geographical Indications*, in *Intellectual Property Institute of Canada*, 2020, p. 33 e seguenti, in cui l'autore evidenzia che l'efficacia della tecnologia blockchain nel mitigare la contraffazione delle Indicazioni Geografiche dipende strettamente dalla legislazione del paese in cui si verifica l'infrazione. Ad esempio, i titolari dei diritti IG sul formaggio FETA, originario della Grecia, potrebbero verificare che l'infrazione viene trattata diversamente in almeno tre giurisdizioni diverse. Negli Stati Uniti, a causa dell'opposizione all'espansione dei diritti IG oltre vino e liquori, sarà molto difficile provare l'infrazione al di fuori dei parametri dell'articolo 22.2 del TRIPS. Pertanto, se il nome FETA viene utilizzato da un produttore di formaggio statunitense, ma l'origine del prodotto è indicata come Stati Uniti e il cliente non viene ingannato, non ci sarà infrazione. In Canada, non ci sarà probabilmente infrazione se il produttore canadese usa qualificatori come "tipo" o "stile di" per indicare che il formaggio non è direttamente associato con il prodotto greco e l'etichetta mostra chiaramente che il prodotto è fabbricato in Canada. Questo orientamento deriva dall'accordo economico di partenariato tra Canada e Unione Europea. Al contrario, nei paesi dei CARIFORUM, l'uso del nome FETA su un prodotto potrebbe costituire infrazione a causa delle robuste disposizioni dell'accordo di libero scambio con l'Unione Europea che vietano l'uso di nomi IG, anche se è indicato il vero luogo di origine, e l'uso di qualificatori come "simile" o "imitazione di". In questi contesti, le capacità di tracciabilità della blockchain possono supportare le rivendicazioni di infrazione prima e durante il contenzioso. Quando esistono differenze nei diritti IG tra giurisdizioni, la tecnologia blockchain ha un impatto limitato sulla

Infatti, qualora si volesse effettuare una modifica di un particolare blocco, tale cambiamento verrebbe memorizzato da un nuovo blocco della catena che rivelerà che è stato introdotto un determinato cambiamento in un determinato momento temporale.
In tal senso la blockchain rappresenta una modalità non distruttiva per iscrivere e tracciare qualsiasi tipo di informazione. Tutti i dati e tutte le modifiche memorizzati su blockchain sarebbero tracciati e non potrebbero andare persi.
Tale sistema permetterebbe una più precisa definizione e verifica delle responsabilità, sia con riferimento all'ambito di produzione, sia con riferimento all'intera *supply chain*, per ciascuna fase di competenza.
Infatti, quando qualcosa non è in linea con i requisiti, ad esempio a causa di prodotti contraffatti, la parte responsabile, più facilmente identificabile all'interno della blockchain, potrebbe essere soggetta a restrizioni, fino all'eliminazione del suo accesso alla blockchain.
In termini di responsabilità, l'ecosistema blockchain è così in grado di promuovere comportamenti diligenti da parte di tutte le entità coinvolte nella catena alimentare.[32]

IV. Promozione della sostenibilità attraverso la blockchain e le indicazioni geografiche

Un altro aspetto che vede un sistema blockchain collimare con la disciplina delle indicazioni geografiche, è quello della sostenibilità.
Infatti non c'è dubbio che nel tempo si è affermata tra i consumatori,[33] e di conseguenza tra le aziende,[34] la tendenza a favorire prodotti di alta qualità coltivati o allevati in modo sostenibile, spesso ad indicazione geografica.
La sostenibilità, in particolare, è stata un tema fortemente discusso negli ultimi anni a causa delle sfide future che attendono il nostro pianeta. Oggi, infatti, molti consumatori

protezione dei diritti IG a livello transnazionale. Un aspetto critico riguarda infatti le diverse definizioni di IG tra le giurisdizioni. Ad esempio, sotto il Trademarks Act canadese, le IG sono identificate come prodotti agricoli e alimentari, o vini e liquori, mentre in paesi come India e Svizzera, le IG possono includere beni agricoli, naturali, manifatturati o prodotti farmaceutici. Sebbene la tecnologia blockchain possa identificare un prodotto come non conforme a un sistema di etichettatura blockchain, se il prodotto non è legalmente identificabile come IG nel paese ospitante, la tecnologia non offre benefici aggiuntivi. Quando la protezione delle IG è meno favorevole nelle giurisdizioni estere, si raccomanda quindi un approccio diversificato alla protezione della proprietà intellettuale per mitigare le perdite. Se i titolari dei diritti IG possono registrare i loro diritti come marchi in regimi restrittivi per le IG, si ottiene un livello di protezione contro le infrazioni relative ai marchi in questi mercati. In questo contesto, le tecnologie blockchain possono essere utili nelle rivendicazioni di infrazione per fornire prove di proprietà e autenticità dei prodotti.

[32] In questo senso, si veda: I. Hernandez, L. G. Vaqué, *The Blockchain Technology and the Regulation of Traceability: The Digitization of Food Quality and Safety*, in *the European Food and Feed Law Review (EFFL)*, 2021, Vol. 15, No. 6, pp. 563 e seguenti, i quali sottolineano come, in termini di responsabilità, l'ecosistema blockchain possa promuovere comportamenti onesti da parte di tutte le entità coinvolte nella catena alimentare.

[33] Sul punto, si veda: J. Qian, L. R. Garcia, B. Fan, J. I. R. Villalba, *Food traceability system from governmental, corporate, and consumer perspectives in the European Union and China: A comparative review*, in *Trends in Food Science & Technology Journal*, 2020, Vol. 99, No. 4, pp. 407 e seguenti, in cui gli autori affermano che l'implementazione corretta dei sistemi di tracciabilità alimentare (FTS) ha un impatto positivo sull'esperienza del consumatore in quanto migliora la fiducia del consumatore riguardo all'origine e alla qualità del prodotto.

[34] Sul punto, si veda: M. Garaus, H. Treiblmaier, *The influence of blockchain-based food traceability on retailer choice: The mediating role of trust*, in *Food Control Journal*, 2021, Vol. 129, pp. 1 - 12, i quali evidenziano come il sistema di tracciabilità basato su blockchain (rispetto a un sistema di tracciabilità di proprietà dell'azienda) abbia un impatto positivo sulla scelta del rivenditore; e L. Dong, P. Jiang, F. Xu, *Impact of Traceability Technology Adoption in Food Supply Chain Networks*, in *Management Science*, 2020.

ritengono essenziale che il cibo sia prodotto in modo sostenibile nel rispetto dell'ambiente e degli "Obiettivi di Sviluppo Sostenibile" (SDGs) dell'Agenda 2030 delle Nazioni Unite.[35] Così come con la blockchain è possibile intervenire per la conformità agli standard IG, allo stesso modo sarà possibile intervenire per la conformità ad altri standard: biologico, non-OGM, allevamento all'aperto o alimentazione ad erba, etc.[36]

Un sistema di questo tipo che valorizza le indicazioni geografiche potrebbe essere una soluzione efficace e trasparente per attestare la sostenibilità dei prodotti ad indicazione geografica che hanno seguito un processo tale da determinare una riduzione di sprechi e di inefficienze.

Nella maggior parte dei casi, esiste una grande distanza tra produttori e consumatori. L'accesso al cibo sano e nutriente si basa sul diritto alla sovranità alimentare,[37] che premia forme di agricoltura virtuose e rigenerative, e presta attenzione ai bisogni della terra e di tutte le forme di vita coinvolte: risorse umane e risorse naturali.

L'utilizzo del sistema blockchain aiuterebbe a colmare la suddetta distanza e a valorizzare

---

[35] Il 14º sondaggio annuale sull'Alimentazione e la Salute (2019) della Fondazione International Food Information Council (IFIC) ha rilevato che il 54% dei consumatori americani afferma che "è almeno in qualche misura importante che i prodotti che acquistano siano prodotti in modo ecologicamente sostenibile. Tra questi, molti cercano etichette o attributi specifici per valutare se un prodotto possa ritenersi ecologicamente sostenibile: il 51% percepisce i prodotti prodotti localmente come ecologicamente sostenibili, seguiti dai prodotti letteralmente etichettati come prodotti in modo sostenibile (47%), etichettati come non OGM/non bioingegnerizzati (47%), etichettati come biologici (44%), con imballaggi riciclabili (41%) e con imballaggi minimali (35%)". Sondaggio ufficiale disponibile su: https://foodinsight.org/wp-content/uploads/2019/05/2019-Food-and-Health-Survey-release-FINAL.pdf (2021). Il sondaggio dell'Organizzazione Europea dei Consumatori sulle attitudini dei consumatori europei verso il cibo sostenibile rivela che oltre la metà dei consumatori europei afferma che "le preoccupazioni sulla sostenibilità hanno una certa influenza (42,6%) o molta influenza (16,6%) sulle loro abitudini alimentari. Oltre un terzo dei consumatori (38,9%) sarebbe favorevole a regolamenti che obblighino agricoltori e produttori alimentari a rispettare standard di sostenibilità più rigorosi. Ancora di più (53%) concordano sul fatto che gli agricoltori dovrebbero ricevere incentivi (ad esempio, attraverso sussidi) per produrre cibo in modo più sostenibile. E infine, la maggior parte dei consumatori (57%) vuole che le informazioni sulla sostenibilità siano obbligatorie sulle etichette alimentari". Sondaggio ufficiale disponibile su: https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-042_consumers _and_the_transition_to_sustainable_food.pdf. Per quanto riguarda le opportunità legate all'applicazione della blockchain all'agricoltura, in termini di tracciabilità, salute e sostenibilità, si veda: H. KIM, M. LASKOWSKI, *Agriculture on the Blockchain: Sustainable Solutions for Food, Farmers, and Financing*, in D. Tapscott (ed.), *Supply Chain Revolution: How Blockchain Technology Is Transforming the Global Flow of Assets*, Barlow Publishing, Toronto, 2018, p. 67 e seguenti; D. FRIEDMANN, *Protecting the Integrity of Consumer Information and the Supply Chain of Wine in China*, in F. D. Simões (ed), *Consumer Protection in China: Current Challenges and Future Prospects*, Brill, Leiden, 2020; N. POPPER, S. LOHR, *Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?*, in The New York Times, 2017. Per ulteriori informazioni sulle peculiarità della blockchain, con una lettura orientata alla regolamentazione tramite la tecnologia, si veda: P. FILIPPI, A. WRIGHT, *Blockchain and the law: the Rule of Code*, cit.

[36] In letteratura, si veda: S. M. ARONZON, *Blockchain and geographical indications: a natural fit?*, cit., p. 10, in cui si menziona l'esempio di Gustav Gerig, una società alimentare svizzera che sta utilizzando la blockchain per rendere tracciabile una particolare gamma di tonno certificato sostenibile dalla cattura alla lavorazione finale. Il consumatore può verificare che il tonno è stato catturato in modo sostenibile accedendo ai dati informativi relativi a: "capitano, nave, tempo di cattura, metodo e area, dove e quando è stato lavorato". Iniziative simili sono in corso per tracciare il pesce di origine sostenibile da parte del World Wildlife Fund for Nature.

[37] "Food sovereignty is the right of peoples to healthy and culturally appropriate food produced through ecologically sound and sustainable methods, and their right to define their own food and agriculture systems. It puts the aspirations and needs of those who produce, distribute and consume food at the heart of food systems and policies rather than the demands of markets and corporations." Dichiarazione di Nyéléni, primo Forum globale sulla sovranità alimentare, Mali, 2007. Disponibile su: https://nyeleni.org/DOWNLOADS/Nyelni_EN.pdf.

i pilastri di provenienza, autenticità e qualità a tutela delle piccole e medie imprese locali, affermando la narrazione di ogni prodotto in modo trasparente. E ciò porterebbe il mercato a seguire scelte più autentiche e sostenibili,[38] promuovendo un accesso consapevole alle risorse attraverso l'uso della tecnologia.

V. BLOCKCHAIN E INDICAZIONI GEOGRAFICHE: SFIDE E OPPORTUNITÀ

Nonostante i numerosi vantaggi fin qui evidenziati, l'implementazione della blockchain presenta numerose sfide.

Il primo ostacolo riguarda sicuramente la consapevolezza dei consumatori in merito ai benefici aggiuntivi di un sistema blockchain in parallelo ad un aumento dei prezzi dei prodotti certificati.[39]

D'altra parte, molti operatori del settore alimentare mantengono una certa diffidenza nei confronti di sistemi tecnologici innovativi e complessi, che alterano le pratiche consolidate e comportano costi aggiuntivi. Tuttavia, alcuni hanno colto i benefici che un sistema di tracciabilità basato sulla blockchain potrebbe offrire in termini di sviluppo ambientale, sociale e reputazionale.[40]

L'interoperabilità e i costi del sistema rappresentano ancora delle questioni problematiche su cui gli esperti si stanno confrontando, e che ostacolano l'adozione della blockchain su larga scala.[41]

---

[38] A tal proposito, si veda: A. STAZI, R. JOVINE, *Food Traceability in Europe, the US and China: A Comparative and Technological Analysis*, cit.; e J. FRANK, *Blockchain Functionality: How Smart Contracts Can Save Small Farms*, cit., p. 22, i quali sottolineano che, basandosi su un recente cambiamento nella percezione pubblica a favore delle piccole aziende agricole rispetto alle grandi imprese agricole industriali, negli Stati Uniti, i piccoli produttori dovrebbero incorporare le recenti innovazioni della blockchain e della tecnologia digitale per assumere una maggiore rilevanza per i consumatori, sopravvivendo all'industria delle grandi imprese.

[39] A tal proposito, si veda: M. GARAUS, H. TREIBLMAIER, *The influence of blockchain-based food traceability on retailer choice: The mediating role of trust*, cit., i quali evidenziano che gli studi hanno confermato che i consumatori mostrano preferenze nei confronti dei piccoli produttori e sono disposti a pagare un prezzo maggiorato se gli altri attori della catena di approvvigionamento sono trattati equamente. Un caso di studio condotto dal 5 al 9 novembre 2019 mirava a esaminare l'impatto di un sistema di tracciabilità basato su blockchain rispetto a un sistema di proprietà aziendale sulla preferenza dei consumatori per la scelta del rivenditore. Lo studio ha coinvolto 180 studenti di amministrazione aziendale di due università di Vienna, che hanno partecipato all'esperimento. I partecipanti sono stati esposti a due rivenditori ipotetici: uno utilizzante un sistema di tracciabilità basato su blockchain e l'altro un sistema interno aziendale. I partecipanti hanno completato un questionario per valutare la loro scelta del rivenditore. Ciò includeva una domanda diretta su quale negozio avrebbero preferito per la spesa settimanale e una misura della scelta del rivenditore su una scala codificata. Fattori aggiuntivi come la conoscenza della blockchain e la fiducia dei consumatori nella sicurezza alimentare sono stati anch'essi considerati, ma non hanno influenzato significativamente la scelta del rivenditore. I risultati hanno mostrato una chiara preferenza per il rivenditore con un sistema di tracciabilità basato su blockchain. Nella condizione sperimentale, il 60% ha preferito il rivenditore basato su blockchain (rivenditore A), rispetto al 40% nella condizione di controllo in cui il rivenditore A utilizzava un sistema interno aziendale. L'analisi statistica ha confermato l'impatto significativo del tipo di sistema di tracciabilità sulla scelta del rivenditore, dimostrando un'influenza positiva della tracciabilità tramite blockchain sulla preferenza dei consumatori. Questo risultato è rimasto costante anche dopo aver controllato variabili come la conoscenza della blockchain e la fiducia dei consumatori nella sicurezza alimentare.

[40] La classifica complessiva degli sviluppi internazionali sulla sostenibilità di tutti i 193 Stati membri delle Nazioni Unite è disponibile su: https://dashboards.sdgindex.org/rankings

[41] Si veda: M. MADINE, K. SALAH, R. JAYARAMAN, Y. AL-HAMMADI, *AppXchain: Application-Level Interoperability for Blockchain Networks*, cit., pp. 87777-87789. A tal proposito, l'Amministrazione del Cyberspazio cinese, nel Regolamento sulla Gestione delle Informazioni Blockchain del 2019, ha dichiarato la propria disponibilità a standardizzare i servizi legati alla blockchain, supportare uno sviluppo "sano" della

Tuttavia il tema più rilevante per l'implementazione di una soluzione blockchain per le indicazioni geografiche è rappresentato dalla necessità di un coinvolgimento delle autorità governative/private di controllo per chiudere il cerchio della fiducia nel sistema.
Diverse sono le aziende attualmente già in grado di consentire alle imprese alimentari di condurre auto ispezioni e allo stesso tempo condividere i dati con le autorità.[42]
Tale prospettiva, concretizzabile in una forma di governance blockchain a carattere privato più che pubblico, vedrebbe così il coinvolgimento di produttori, intermediari tecnologici e autorità al fine di garantire il funzionamento del sistema.[43]
Il sostegno delle autorità governative per ammortizzare i costi e favorire il completamento del sistema, assieme al know-how tecnico sulle blockchain, renderebbe così fruibile il sistema ai produttori e andrebbe a beneficio dei consumatori e dei pilastri di provenienza, autenticità e qualità tipici delle indicazioni geografiche.
In conclusione, le politiche di Regulatory Technology dovrebbero incentivare non solo lo sviluppo di tecnologie innovative, ma anche la formazione e sensibilizzazione sugli strumenti il cui potenziale rimane ancora in parte inespresso.
Così facendo, si potrebbe promuovere efficacemente l'adozione di sistemi innovativi capaci di generare benefici significativi per le imprese, indipendentemente dalla loro dimensione, oltre che per i consumatori e l'ambiente, garantendo al contempo il rispetto delle normative vigenti nei diversi ordinamenti giuridici e rivalorizzando l'origine e le tradizioni.

tecnologia e affrontare i rischi di sicurezza, come la diffusione di informazioni illegali e dannose o la conduzione di attività illegali e criminali attraverso questa tecnologia. Disponibile su: https://digichina.stanford.edu/news/translation-blockchain-information-service-management-regulations-2019.

42 J. BARBERIS, D. W. ARNER, R. P. BUCKLEY, *The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*, cit. CoInspect is an example of this application making it easy to manage food safety compliance and brand standards. Platform project available at: https://ww4.mewe.org/#overview. Un altro esempio è rappresentato da Bureau Veritas che, con la sua piattaforma blockchain Origin, mira a favorire l'implementazione di sistemi di tracciabilità alimentare blockchain e l'ideazione di sistemi di governance appropriati a tutela delle indicazioni geografiche. Disponibile su: https://group.bureau veritas.com/newsroom/bureau-veritas-launches-origin-worlds-first-blockchain-based-complete-food-traceability.

43 In tal senso, si veda: S. M. ARONZON, *Blockchain and geographical indications: a natural fit?*, cit., p. 12, in cui l'autrice afferma che un candidato quale intermediario di fiducia potrebbe essere l'OMPI. L'OMPI potrebbe implementare una soluzione blockchain più generale che potrebbe essere personalizzata secondo le necessità dei gruppi di produttori di prodotti ad indicazione geografica. L'OMPI amministra l'Accordo TRIPS (che nell'Articolo 22 definisce uno standard di protezione per le indicazioni geografiche) e copre un vasto territorio di firmatari, quindi appare come un buon candidato per coordinare tale soluzione. Da parte dell'OMPI sarebbe un investimento e un impegno significativo, in quanto una delle funzioni dell'OMPI è aiutare a creare infrastrutture tecniche globali per la proprietà intellettuale e "sviluppare strumenti, servizi, standard, database e piattaforme di proprietà intellettuale condivisi", il che include anche l'indagine sulle potenzialità delle applicazioni blockchain.

RECENSIONE
SULLE SPALLE DEI GIGANTI? LA QUESTIONE METODOLOGICA DEL DIRITTO COMPARATO E IL SUO RACCONTO
(Tommaso Amico di Meane, Napoli:Editoriale Scientifica, 2022, 376 pg.)

Laura Bugatti

INTRODUZIONE

Presentando una ricostruzione diacronica dei metodi convenzionali del diritto comparato, questo libro sostiene che, per qualificare il diritto comparato come disciplina, i comparatisti devono riflettere su come e perché fanno i confronti. L'autore discute non solo i metodi e le teorie, ma anche le implicazioni etiche e politiche del diritto comparato, mettendo in luce le diverse dimensioni della disciplina. L'autore passa così in rassegna i diversi approcci che hanno animato il discorso giuridico proprio del diritto comparato, tra cui l'analisi di un diffuso spirito di innocenza in termini di metodo e la critica delle narrazioni sui diritti umani. Esamina inoltre il modo in cui i tribunali negoziano le differenze tra i casi riguardanti il velo musulmano. Le critiche e i confronti incisivi contenuti in questo libro saranno una lettura essenziale per i comparatisti che lavorano nella formazione e nella ricerca giuridica, così come per gli studenti di diritto comparato e gli studiosi di antropologia comparata e scienze sociali.

In apertura del volume, l'autore descrive il suo progetto esplicitamente come una critica, collocando l'opera nell'ambito delle teorie critiche, che riunisce non pochi studiosi del diritto comparato, in Italia e all'estero. In termini sostanziali, il percorso immaginato dall'autore può essere concepito come una genealogia della disciplina comparatistica tradizionale. Attraverso questa mappatura temporale, nelle diverse fasi analizzate, la comparazione assume molte forme diverse, dal diritto comparato universalista e colonialista delle origini, a quello funzionalista e istituzionale, fino al comparato transnazionale e specialistico della contemporaneità. Questa evoluzione si caratterizza, secondo l'autore, per l'insorgere di una costante dicotomia tra la corrente ortodossa e quella critica, che è situata spazialmente oltre l'occidente, ma in costante collegamento con lo stesso. In questo senso, il diritto comparato ortodosso è composto da una serie di approcci metodologici che si susseguono alla ricerca di soluzioni ottimali alle questioni giuridiche, spesso intesi dal punto di vista dell'Occidente. In contrasto con questa ortodossia, il diritto comparato critico mira a confrontarsi con l'autorità incarnata dalla corrente principale per metterne in discussione le certezze, i metodi, le categorie e svelarne le narrative e la politica.

Uno strumento chiave del progetto dell'autore per ricostruire questo dialogo metodologico interno al diritto comparato è la genealogia. Il passato della disciplina viene così scandagliato per individuare i sentieri più battuti e quelli meno visibili della disciplina allo scopo di restituire la complessità dal discorso giuridico comparatistico, le antinomie e i rapporti tra la scienza ortodossa e quella critica.

L'autore presenta questi due assi come sfide per la comparazione piuttosto che come prove dell'inutilità del diritto comparato. Amico Di Meane concorda sul fatto che valga la

pena imparare a navigare tra i diversi approcci metodologici per comprendere gli attuali confini della comparazione giuridica e di conseguenza per consentire al comparatista di acquisire una maggiore consapevolezza delle implicazioni sociali e politiche delle sue analisi. Questo può essere possibile solo se lo stesso comparatista accetta che le proprie conoscenze consolidate sul diritto sono il prodotto di un sapere tecnico situato in un contesto ideologico ben preciso, deve imparare quindi a differenziare, cioè a vedere il proprio punto di vista in termini particolaristici (anziché universalistici).
Le tre scansioni storiche producono una mappa dei principali passaggi della comparazione giuridica. Il filo rosso che collega questi momenti è rappresentato da una tendenza del diritto comparato ortodosso a porre una certa enfasi sulla dicotomia differenza / somiglianza, che accompagna da sempre la comparazione. Questo strumento epistemologico, rinvenibile nei maggiori approcci metodologici (funzionalismo e strutturalismo ad esempio) e nelle tassonomie del diritto comparato, sembra non essere turbato dalle rivendicazioni di etnocentrismo e da altre difficoltà illustrate dall'opera di Amico di Meane. Invece dell'introspezione metodologica, questo filone del diritto comparato mira a stabilire un controllo cognitivo sul diritto straniero, allo scopo di condurre i propri (celati) obiettivi politici, quali ad esempio l'armonizzazione giuridica. Un'altra tendenza della scienza comparatistica è quella di perseguire una ricerca universalistica di esperienze giuridiche condivise a livello globale. L'approccio universalista è evidente negli sforzi per costruire un diritto mondiale universale e nei tentativi più modesti di ampliare gli orizzonti degli studenti di diritto attraverso corsi di diritto comparato, questi due progetti - controllo cognitivo e universalismo - costituiscono l'ideologia inconscia del diritto comparato mainstream.
Un approccio scientificamente più marginale, ma alquanto diffuso all'interno del diritto comparato, come si può evincere dal volume, combina l'analisi meramente tecnico-giuridica, lo studio specialistico di determinate tematiche e la sostanziale indifferenza alle questioni metodologiche. A differenza dei primi due esempi di comparazione giuridica, questa tendenza non è collegata a nessun progetto politico particolare, se non quello di dimostrare la congenita neutralità e la sostanziale oggettività del sapere giuridico. In questo caso, l'esaltazione del distacco metodologico e della differenza produce uno scetticismo paralizzato sulla comparazione quale terreno prettamente tecnico. A questo approccio si può ricondurre anche quella componente della comparazione che si astiene dallo studio di esperienze giuridiche provenienti da tradizioni più lontane da quelle europee, come sottolinea perspicacemente l'autore, gli scettici che operano nel campo del diritto comparato hanno affrontato queste difficoltà metodologiche semplicemente rifiutando di confrontarsi con le prospettive non occidentali.

II. UN METODO CRITICO PER RACCONTARE IL METODO: LA GENEALOGIA

Il percorso genealogico proposto da Amico di Meane cerca di rivelare le forze che sono represse nei resoconti ortodossi del diritto comparato. Il volume consegna al lettore l'immagine del comparatista destinato a enfatizzare o a sminuire le metodologie della comparazione giuridica. Per esempio, un comparatista è sempre o troppo distante dal diritto straniero che sta analizzando o troppo coinvolto dallo stesso - non c'è un modo

giusto per farlo. Lo studio è così particolarmente utile perché mette in luce le possibili strade che sono comprese all'interno della disciplina: quella che comprime le differenze, quella che le esalta e quella critica delle prime due. L'autore accompagna il lettore attraverso una serie di esperienze storiche che coinvolgono i comparatisti come in un multiverso nel quale è impossibile non perdere la strada di casa. Il lettore impara secondo un procedimento di *trial and error* dai racconti del passato, comprendendo che non vi sono che approcci perfettibili e conoscenze parziali.

Se da un lato *Sulle spalle dei giganti?* si scaglia contro i luoghi comuni del diritto comparato tradizionale, dall'altro il libro è scritto da un osservatore a cui interessa prendere parte all'azione. In modo insolito per uno studioso critico, l'autore costruisce un difficile dialogo tra gli studiosi comparatisti tradizionali e i loro critici, impegnandosi a dimostrare ad altri giuristi comparatisti come questa relazione sia sopravvissuta in tutte le fasi della breve storia della disciplina. Di conseguenza, l'autore è un critico particolarmente comprensivo per gli standard della critica giuridica: si relaziona alle diverse esperienze con il solito intento di farne emergere insegnamenti e non giudizi a posteriori. *Sulle spalle dei Giganti?* è anche ideologicamente attento, nel senso che non avanza alcuna agenda politica specifica, il che potrebbe risultare sgradevole per i comparatisti tradizionali, ma si limita a illustrare quelle che sono state impiegate nel corso degli anni.

Invece di sostenere un particolare approccio ideologico, l'autore si unisce allo sforzo comune dei comparatisti di affrontare e comprendere diritti stranieri e culture giuridiche diverse. Nel perseguire questo obiettivo, il diritto comparato impiega molti strumenti metodologici tradizionali e qualche strumento critico. Leggendo le pagine del volume, sembra inoltre che l'Occidente sia una categoria importante sia per il diritto comparato tradizionale che per quello critico, anche se per ragioni diverse. L'autore utilizza questo concetto per decostruire l'eurocentrismo e l'etnocentrismo nel diritto comparato e provincializzare il diritto occidentale. Egli critica la tendenza degli studi storici comparati a incorporare invariabilmente la prospettiva occidentale e a costruire il mondo a partire da questa. Il volume fa emergere come uno dei filoni del diritto comparato tradizionale opera nel quadro della distinzione binaria tra rilevante o principale e non così rilevante, quasi un corollario alla dicotomia tra differenze e somiglianze. Si tratta di una prospettiva critica davvero interessante. Tuttavia, la costruzione stessa del libro di Amico di Meane, la sua trattazione e gli oggetti rilevanti o principali della sua critica, così come il suo pubblico, sono situati in Occidente. La pratica del distanziamento, ad esempio, è intesa a trovare un "equilibrio tra il diventare nativi e il rimanere occidentali". Negare l'eurocentrismo può finire per affermarlo.

III.. LE METODOLOGIE COMPARATISTICHE COME SCELTE STRATEGICHE

Il fatto che il volume si concentri sull'esperienza occidentale del diritto comparato ha senso, dato che l'origine dell'eurocentrismo non può che essere rintracciata in Occidente. Una maggiore autocomprensione può avviare un processo di dialogo critico, come sottolinea Amico di Meane. L'incontro del diritto comparato con l'Altro e, in particolare,

con il non Occidente, non può che avvenire sulla base di una conoscenza perfetta non tanto dell'ordinamento o dell'istituto a cui si fa riferimento, ma dei limiti al sapere che si sceglie di impiegare nella comparazione stessa. I giuristi e i teorici del diritto e i comparatisti hanno avuto interazioni fruttuose solo nella consapevolezza dei rispettivi confini culturali percepiti. Il diritto comparato (come disciplina collettiva) può essere in grado di mappare i contorni della propria disciplina così come sono stati identificati da Amico di Meane?

In effetti, si può individuare una via d'uscita da questo intreccio all'interno del volume. *Sulle spalle dei giganti?* Dimostra come le metodologie comparatistiche, che si sono sempre basate sull'impiego di una dicotomia differenza / somiglianza possono, in fin dei conti, essere comprese solo se le si concepisce come scelte strategiche. I tre capitoli del libro non sono solo un'analisi diacronica degli studi comparatistici, rappresentano un catalogo di strategie geopolitiche del diritto, sono particolarmente efficaci come critiche ai principi omogeneizzanti del diritto comparato perché accettano il suo uso strategico, la sua funzionalizzazione a scopi ulteriori di matrice politica. Si tratta di osservazioni che fanno riflettere e che sono ben lontane dal regno idilliaco del diritto comparato, anzi lo situano storicamente e culturalmente, ne fanno un oggetto di studio materialistico che lo spoglia degli orpelli tradizionali.

In conclusione, questo volume costringe i giuristi comparatisti a riflettere a fondo sui loro metodi, sulla loro politica e sulla storia della loro disciplina. Perché comparare? E, cosa altrettanto importante, l'autore dimostra che in alcuni casi la sensibilità comparatistica svia le ricerche degli studiosi. Sarebbe un peccato se il progetto di stabilire e colmare i divari tra il "vicino" e il "lontano", il "familiare" e lo "straniero" dissuadesse i comparatisti dall'impegnarsi in dibattiti che sono, probabilmente, sia a livello globale che municipale più rilevanti delle comparazioni giuridiche e delle loro critiche. Questo è l'ultimo messaggio dell'autore ai suoi compagni di studi: i giuristi comparatisti devono impegnarsi nei dibattiti incontrando altri diritti e pratiche giuridiche consapevoli delle proprie ideologie e delle conseguenti strategie. I potenziali visitatori della terra del diritto comparato dovrebbero leggere il libro questo volume prima di intraprendere il viaggio.