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

6
CAMILLA CREA – BIANCA GARDELLA TEDESCHI
Il concepito e l'aborto: una comparazione critica tra Italia e Perù

27
PAOLO GUARDA – RAZMIK VARDANIAN
Certifications and protection of personal data: an in-depth analysis of a powerful compliance tool

56
MARINA FEDERICO
On Lands and Dispossession. The Relevance and Potential of Property Law for the Constitutional Recognition of the Rights of Indigenous Peoples

85
ANDREA STAZI
Late Payments in the Construction Industry: Comparative Law and Policy Approach in the UAE

95
FEDERICA GIOVANELLA
L'aspettativa di privacy del lavoratore: prospettive di diritto comparato

130
ISABELLA FERRARI
Tutela della proprietà intellettuale nel mondo dell'intelligenza artificiale: Artificial Inventor Project, Thaler e i brevetti negati a Dabus

147
RICCARDO IOVINE
Innovazione e tradizione: RegTech, Blockchain e indicazioni geografiche

162
RECENSIONE
“Sulle spalle dei giganti?
La questione metodología del diritto comparato e il suo racconto”

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.