IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
Anno XXIX Fasc. 1 - 2013

Federica Giovanella

IMMAGINI PEDOPORNOGRAFICHE, PRIVACY DEL LAVORATORE E PROTEZIONE COSTITUZIONALE: IL PUNTO DELLA CORTE SUPREMA CANADESE

Estratto

Milano • Giuffrè Editore

CORTE SUPREMA
DEL CANADA
19 OTTOBRE 2012

GIUDICI: MCLACHLIN, LEBEL

PARTI: HER MAJESTY THE QUEEN, COLE

Privacy sul luogo di lavoro
• Detenzione di materiale pedopornografico
• Ispezioni e sequestri di computer senza mandato
• Violazione di un interesse costituzionale alla privacy
• Sussistenza

Sussiste una ragionevole aspettativa di privacy del lavoratore sulle informazioni contenute in un computer di lavoro utilizzato anche per scopi personali. Conseguentemente, ai sensi della sezione 8 della Canadian Charter of Rights and Freedoms, *è illecita l'ispezione da parte di un agente di polizia avvenuta senza mandato, a nulla rilevando l'eventuale consenso del terzo/datore di lavoro proprietario del computer in questione.*

Justice Fish:

In *R. v. Morelli* (2010 SCC 8, [2010] 1 S.C.R. 253) la Corte Suprema non lasciò dubbi circa il fatto che i Canadesi possono aspettarsi di avere privacy sulle informazioni contenute nei loro computer personali. Nella mia opinione, lo stesso ragionamento si applica alle informazioni contenute nei computer di lavoro, quantomeno quando un uso personale degli stessi è permesso o almeno supposto.

I computer che siano ragionevolmente utilizzati per scopi personali — indipendentemente che siano trovati sul posto di lavoro o a casa — contengono informazioni che sono significative, intime e pertinenti il nucleo biografico dell'utilizzatore. Nei confronti dello stato, ciascuno in Canada è costituzionalmente titolato ad attendersi della riservatezza nelle informazioni personali di questo tipo.

Sebbene le norme interne e le pratiche del posto di lavoro possano diminuire l'aspettativa di privacy che un individuo ha su un computer di lavoro, questo tipo di realtà operative non rimuovono di per sé totalmente l'aspettativa: la natura delle informazioni in gioco espone preferenze, interessi, pensieri, attività, idee e ricerche d'informazioni dell'utente.

Questo accadeva nel caso in esame. Al signor Cole, un insegnante di scuola superiore, era permesso di utilizzare il suo computer di lavoro per incidentali scopi personali. Egli lo fece. Navigò in internet e immagazzinò informazioni personali sul suo disco fisso.

Un tecnico, mentre effettuava attività di manutenzione, trovò sul computer portatile del signor Cole una cartella nascosta contenente foto di una studentessa nuda e parzialmente nuda. Il tecnico informò il preside e, sotto la direzione di quest'ultimo, copiò le fotografie su di un *compact disc* (CD). Il preside sequestrò il computer e i tecnici della scuola copiarono i file temporanei di Internet su un secondo CD. Il computer ed entrambi i CD furono consegnati alla polizia, che, senza mandato, esaminò i loro contenuti e creò una copia identica (*mirror image*) del disco fisso per scopi investigativi.

Il signor Cole fu imputato per possesso di pedo-pornografia e utilizzo non autorizzato di un computer [...] e processato con rito sommario. Il giudice di prima istanza escluse tutti i materiali provenienti dal computer sulla base delle sezioni 8 e 24(2) della *Canadian Charter of Rights and Freedoms*. [...]

La Corte d'appello del rito sommario ribaltò la decisione del giudice di prime cure, ritenendo che non vi fosse violazione della sezione 8 ((2009), 190 C.R.R. (2d) 130 (Ont. S.C.J.)). La Corte d'appello dell'Ontario annullava tale decisione ed escludeva il disco contenente i file temporanei di Internet, il computer portatile e la copia esatta del disco fisso (2011 ONCA 218, 105 O.R. (3d) 253 (Ont. C.A.)).

Io sono d'accordo con la Corte d'Appello sul fatto che la polizia abbia violato i diritti del signor Cole protetti dalla sezione 8 della Carta. Egli si attendeva una certa privacy sulle sue informazioni personali contenute nel computer. Anche tenendo in considerazione le policies del posto di lavoro rilevanti, in tali circostanze tale aspettativa era ragionevole. Era, comunque, un'*aspettativa ridotta di privacy* se comparata con l'interesse alla privacy considerato nel caso Morelli, che, diversamente da questo caso, coinvolgeva un personal computer che apparteneva al signor Morelli e che fu ispezionato e sequestrato in casa sua.

Una ragionevole, anche se ridotta, aspettativa di privacy è comunque un'aspettativa ragionevole di privacy protetta dalla sezione 8 della Carta. Di conseguenza, è soggetta all'intrusione statale solo con l'autorità di una legge ragionevole.

In questo caso la Corona non poteva indicare alcuna legge che autorizzasse la polizia a fare, come fece, un'ispezione del computer di lavoro del signor Cole senza mandato. L'autorità legale del suo datore di lavoro — un consiglio d'istituto — di requisire e ispezionare il computer portatile non forniva alla polizia lo stesso potere. E il « consenso di terzo » del consiglio di istituto all'ispezione non aveva conseguenze legali. [...]

L'utilizzo del computer potatile del signor Cole era regolato dal « Policy and Procedures Manual » del consiglio d'istituto, che permetteva un utilizzo personale incidentale delle tecnologie informatiche del consiglio. Le *policy* stabilivano che la posta elettronica degli insegnanti rimaneva privata, ma soggetta ad accesso da parte degli amministratori della scuola a determinate condizioni. Non parlava di privacy in altri tipi di *files*, ma statuiva che « tutti i dati e i messaggi generati da o gestiti con attrezzature dell'istituto devono considerarsi proprietà del consiglio d'istituto ».

Ci sono prove anche che l'« Acceptable Use Policy » della scuola — scritto per gli studenti e sottoscritto dagli stessi — si applicava *mutatis mutandis* agli insegnanti. Questa *policy* non solo restringeva gli usi che dei computer portatili gli studenti potevano fare, ma avvertiva anche gli utenti di non attendersi riservatezza nei loro *files*.[...]

In nessun momento l'ufficiale di polizia ottenne un mandato per ispezionare il disco fisso del computer o uno dei compact disc.

[...] Il signor Cole impugnò con successo davanti la Corte d'Appello dell'Ontario. La Corte d'Appello ritenne che il signor Cole avesse una ragionevole aspettativa di privacy sul contenuto informazionale del computer, ma che questa aspettativa « era modificata nel senso che il signor Cole sapeva che i tecnici del suo datore di lavoro potevano accedere e avrebbero avuto accesso al computer quale parte del loro ruolo di mantenere l'integrità tecnica della rete informatica della scuola ». [...]

La Corte d'Appello concluse che l'ispezione e il sequestro del computer da parte del preside e del consiglio d'istituto era autorizzata dalla legge e ragionevole. Il disco contenente le fotografia fu dunque creato senza vilare la sezione 8. [...]

Il computer e il disco con i file temporanei di Internet del signor Cole, però, comporta differenti considerazioni. Il signor Cole aveva una conti-

nuativa ragionevole aspettativa di privacy sui suoi materiali, e la loro perquisizione da parte degli ufficiali della scuola non dotava la polizia della *loro* autorità. E la scuola non poteva nemmeno dare il consenso all'ispezione della polizia. Dato che la polizia non aveva altro potere legale, si realizzò una violazione della sezione 8.

La Corte d'Appello escluse il computer portatile e la copia del disco fisso, ai sensi della sezione 24(2) della Carta. […] La Corona impugnò la decisione. […]

Quest'impugnazione solleva [le seguenti] questioni: 1) se la Corte d'Appello errò nel concludere che il signor Cole aveva una ragionevole aspettativa di privacy nel computer fornitogli dal datore di lavoro; 2) se la Corte d'Appello errò nel concludere che l'ispezione e il sequestro del computer e del disco contenente i file di Internet da parte della polizia era irragionevole secondo il significato della sezione 8 della Carta […].

La sezione 8 della Carta garantisce a ciascuno in Canada il diritto ad essere sicuri nei confronti di irragionevoli perquisizioni o sequestri. L'ispezionare è una perquisizione, e il prendere è un sequestro, quando una persona abbia un interesse ragionevole alla privacy in ciò che sia oggetto di tali azioni o nelle informazioni cui ciò dà accesso. […]

La privacy è una questione di aspettative ragionevoli. Un'aspettativa di privacy attrae la protezione della Carta se ragionevole, e se persone informate, trovatesi nella posizione dell'accusato, si aspetterebbero privacy […].

Quando, come in questo caso, un'ispezione è effettuata senza un mandato, è presuntivamente irragionevole […]. Per dimostrare la ragionevolezza, la Corona ha l'onere di provare 1) che l'ispezione era autorizzata dalla legge; 2) che la legge autorizzante era ragionevole di per sé; e 3) che l'autorità che ha effettuato l'ispezione lo fece in modo ragionevole […]

Se il signor Cole avesse un'aspettativa ragionevole di privacy dipende da la « totalità delle circostanze » […].

Il test della « totalità delle circostanze » è un test di sostanza e non di forma. Quattro tipi di indagine guidano l'applicazione del test: 1) una valutazione del materiale esaminato dalla presunta ispezione; 2) una decisione riguardante la possibilità che il ricorrente avesse un interesse diretto nel materiale; 3) un'indagine riguardo all'eventuale soggettiva aspettativa di privacy del ricorrente nel materiale; e 4) un giudizio che stabilisca se l'aspettativa di privacy fosse oggettivamente ragionevole, avendo riguardo alla totalità delle circostanze. Discuterò ciascun punto di seguito.

In questo caso, il materiale esaminato dalla presunta ispezione sono i dati, o contenuti informazionali del disco fisso del computer, e i file di Internet, non quindi i dispositivi in sé stessi.

Il nostro interesse è quindi nell'*informational privacy*: « Il diritto di individui, gruppi o istituzioni di determinare per sé quando, come, e in che modo, informazioni che li riguardano siano comunicati ad altri » […].

L'interesse diretto e l'aspettativa soggettiva di privacy del signor Cole nel contenuto informazionale del suo computer possono essere agevolmente inferite dal suo utilizzo del computer per navigare in Internet e per immagazzinare informazioni personali sul disco fisso.

La domanda rimanente è se l'aspettativa soggettiva del signor Cole fosse oggettivamente ragionevole […].

Nel promuovere i sottostanti valori di dignità, integrità ed autonomia, è appropriato che la sezione 8 della Carta cerchi di proteggere un nucleo biografico di informazioni personali che gli individui in una società libera

e democratica desidererebbero sostenere e controllare dalla diffusione allo stato. Questo includerebbe informazioni che tendono a rivelare dettagli intimi dello stile di vita di una persona e scelte personali dell'individuo.

Più il materiale oggetto di ispezione è vicino al nucleo biografico delle informazioni personali, più questo fattore favorirà una ragionevole aspettativa di privacy. Per dirla in altro modo: più le informazioni sono personali e confidenziali, più canadesi ragionevoli ed informati saranno disposti a riconoscere l'esistenza di un interesse costituzionalmente protetto alla privacy [...].

Questo tipo di informazioni private è il vero cuore del « nucleo biografico » protetto dalla sezione 8 della Carta.

Come in *Morelli* (R. v. Morelli, 2010 SCC 8), questo caso coinvolge informazioni fortemente rivelative e significative della vita personale dell'individuo — un fattore fortemente indicativo di un'aspettativa di privacy ragionevole. Diversamente da *Morelli*, tuttavia, questo caso riguarda un computer *di lavoro* e non un computer trovato in un domicilio privato.

Il « Manuale di policy e procedure » del consiglio d'istituto afferma la proprietà (della scuola) non solo dell'*hardware*, ma anche dei dati contenuti nello stesso (computer). [...]

Nonostante la titolarità della proprietà sia una considerazione rilevante, non è determinante. [...] Le *policies*, le pratiche e gli usi del luogo di lavoro sono rilevanti in tanto in quanto concernono l'uso di computer da parte de lavoratori. Queste « realtà operative » possono diminuire la ragionevole aspettativa di privacy che i dipendenti possono altrimenti avere nelle loro informazioni personali [...].

In questo caso le realtà operative del luogo di lavoro del signor Cole spingono contemporaneamente a favore e contro l'esistenza di un'aspettativa di privacy ragionevole. *A favore*, perché le policy scritte e la pratiche di fatto permettevano al signor Cole di utilizzare il suo computer portatile di lavoro per scopi personali. *Contro*, perché sia le *policy* che la realtà tecnologica lo privavano dell'esclusivo controllo su — e accesso a — le informazioni personali che egli scelse di immagazzinare sul computer [...].

Il preside ricordava ogni anno agli insegnanti che le « Acceptable Use Policy » si applicavano anche a loro. Le policy statuivano che « insegnanti e amministratori possono monitorare il lavoro di tutti gli studenti, nonché le e-mail, compreso il materiale salvato sui dischi fissi dei computer portatili » e che « gli utenti non dovrebbero ritenere che i file immagazzinati nei server della rete o nei dischi fissi dei computer individuale resteranno privati ».

La « totalità delle circostanze » consiste di molti elementi, che in questo spingono in direzioni opposte. A conti fatti, tuttavia, essi supportano l'oggettiva ragionevolezza della soggettiva aspettativa di privacy del signor Cole.

La natura delle informazioni in gioco favorisce pesantemente il riconoscimento di un interesse costituzionalmente protetto alla privacy. L'uso personale da parte del signor cole del suo computer di lavoro generò informazioni che sono significative, intime, e biologicamente connesse al suo nucleo biografico. Di certo, spingono nell'altra direzione l'appartenenza del computer al consiglio d'istituto, le *policy* e pratiche del luogo di lavoro, e la tecnologia presente a scuola. Queste considerazioni diminuiscono l'interesse alla privacy del signor Cole nel suo computer portatile [...] ma non lo eliminano interamente.

Dato che il signor Cole aveva un'aspettativa ragionevole di privacy sulla sua cronologia di Internet e sulle informazioni contenute nel computer di lavoro, ogni esame effettuato da parte dello stato senza il consenso (del signor Cole) deve considerarsi « un'ispezione » e ogni apprensione « un sequestro ». […]

[C]oncordo con la Corte D'Appello. Il preside aveva un obbligo giuridico di mantenere la sicurezza nell'ambiente scolastico e, quale necessaria implicazione, un ragionevole potere di ispezionare e sequestrare un computer della scuola se egli riteneva, su basi ragionevoli, che il disco fisso contenesse foto compromettenti di una studentessa. […]

La questione irrisolta della presente impugnazione è se l'autorità degli ufficiali della scuola concesse *alla polizia* l'autorità legale di condurre un'ispezione e una perquisizione senza mandato. Secondo me, così non fu […].

Certamente, il consiglio d'istituto era legalmente titolato ad informare la polizia della sua scoperta di materiale illecito sul computer. Questo avrebbe indubbiamente permesso alla polizia di ottenere un mandato per ispezionare il computer per il materiale. Ma il fatto di aver ricevuto il computer dalla scuola non autorizzava alla polizia un accesso *senza mandato* alle informazioni personali ivi contenute. Queste informazioni rimanevano soggette, tutto il tempo, alla sussistente aspettativa ragionevole di privacy del signor Cole.

La Corona sostiene una seconda giustificazione per la condotta della polizia: il consenso del terzo. La Corona sostiene che il datore di lavoro (un terzo) può validamente acconsentire ad un'ispezione e perquisizione senza mandato su un computer concesso ad uno dei suoi dipendenti. La premessa sottostante è che un terzo può rinunciare all'interesse di privacy del terzo — facendo così venir meno la garanzia di quella persona ai sensi della sezione 8 della Carta. […]

[L]a dottrina del consenso del terzo è incoerente con la giurisprudenza di questa Corte sul consenso dell'interessato […] Perché il consenso sia valido, deve essere al contempo volontario ed informato. L'adottare una dottrina del consenso del terzo in questo Paese implicherebbe che la polizia potrebbe interferire con l'interesse alla privacy di un individuo sulla base di un consenso *non* volontariamente dato dal titolare del diritto, e *non* necessariamente fondato su sufficienti informazioni nelle sue mani per poter compiere una scelta significativa.

Immagini pedopornografiche, privacy del lavoratore e protezione costituzionale: il punto della Corte Suprema canadese

1. Il caso.

Con la sentenza in esame la Corte Suprema del Canada prende posizione circa l'aspettativa di privacy che un lavoratore può legittimamente avere nelle informazioni personali rinvenibili sul luogo di lavoro, con particolare riferimento ad ispezioni e perquisizioni effettuabili dalle forze di polizia. La decisione contribuisce a delineare il diritto alla privacy così come tutelato dalla Sezione 8 della *Ca-*

nadian Charter of Rights and Freedoms[1], affiancandosi al precedente *leading case R. v. Morelli*[2]. L'analisi effettuata nell'opinione di maggioranza appare logica e lucida, pur coinvolgendo numerosi aspetti del diritto alla riservatezza dalle intrusioni statali e giungendo a conclusioni differenti da quelle a cui, come si vedrà, la giurisprudenza maggioritaria era sino ad allora pervenuta.

Questa sentenza può essere considerata come principio di cambiamento: se fino ad oggi era prevalente la presunzione che un dipendente non potesse avere un'aspettativa ragionevole di privacy in relazione alle informazioni contenute in un computer di lavoro, con questa decisione la Suprema Corte chiarisce che si deve avere riguardo alle *policies*, alle pratiche e agli usi che governano l'utilizzo di tale tecnologia.

2. Il diritto alla privacy nel sistema canadese, con particolare riferimento ai lavoratori.

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[3].

Lo scenario è stato modificato profondamente nel 2001, con l'intervento federale del *Personal Information Protection and Electronic Documents Act* (PIPEDA)[4]. La novità introdotta da questo testo è principalmente quella del suo ambito di applicazione: con il PIPEDA, infatti, la raccolta, l'uso e la diffusione di informazioni personali sono per la prima volta regolamentate anche nel settore privato[5]. Per informazione personale si intende un'informazione che riguardi un individuo identificabile, pur non includendo il nome, il titolo, l'indirizzo lavorativo o il numero di telefono di un soggetto impiegato in un'organizzazione, termine che comprende associazioni, imprese, datori di lavoro individuali o sindacati[6]. Ciò significa che informazioni differenti da quelle elencate,

[1] La *Canadian Charter of Rights and Freedoms* è un *bill of rights* contenuto nel *Constitution Act* del 1982 (con cui il Canada raggiunse la piena autonomia politica dal Regno Unito). Con l'introduzione di questa Carta, i diritti ivi contenuti ottengono lo *status* di legge costituzionale, così da superare ogni previsione legislativa federale o statale con cui entrino in contrasto.

[2] *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253.

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

[4] 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 et Al., *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.

[5] 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).

[6] PIPEDA, sez. 2(1) - Definitions.

anche se inerenti lavoratori, saranno soggette ai vincoli stabiliti dal PIPEDA[7].

L'*Act* prevede che ogni raccolta, utilizzo e diffusione di informazioni personali possa avvenire solo per scopi che una « reasonable person » considererebbe appropriati nel caso concreto[8]. 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[9]. In secondo luogo, la normativa in discorso obbliga ciascuna organizzazione a designare un soggetto responsabile della conformità dell'organizzazione alle normative sulla privacy[10]: 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[11]. Inoltre, le varie previsioni sul consenso alla raccolta dei dati, nonché sui limiti e le finalità di quest'ultima[12], pongono dei margini alle possibilità 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 ad essere applicabili, pur in presenza di un'omnicomprensiva disciplina quale il PIPEDA, laddove le stesse siano « sostanzialmente simili » a quest'ultima[13].

---

[7] J. deBeer, *Employee Privacy: the Need for Comprehensive Protection*, cit., 410; G. Lasprogata, N.J. King, S. Pillay, *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, in 2004 *Stanford Technology Law Review* 4, par. 96.

[8] 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*.

[9] 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)).

[10] PIPEDA, Schedule 1, Principle 4.1 - Accountability.

[11] M. Geist, *Computer and E-Mail Workplace Surveillance In Canada*, cit., 23.

[12] 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)).

[13] 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

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[14]. 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[15], il cui ambito di applicazione è tuttavia ristretto alle istituzioni governative federali[16].

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[17]. 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[18].

---

dei lavoratori fra le diverse province J. DEBEER, *Employee Privacy: the Need for Comprehensive Protection*, cit., 407-408; A. LEVIN, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, in 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.

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

[15] R.S.C. 1985, c. H-6.

[16] 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.

[17] 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*, in 48 *California Law Review* 383 (1960), 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).

[18] LEVIN, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, cit., 205. Per una panoramica della protezione della privacy per legge 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*, in 44 *McGill L. J.* 849

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. Sarà pertanto difficilmente utile a proteggere i cittadini per la circolazione di informazioni nel settore privato[19].

Sebbene nella *Charter* non vi sia una previsione specifica a tutela della privacy[20], essa è ricondotta alle sezioni 7 e 8[21]. La prima 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[22]. Più di recente, tuttavia, la lesione della riservatezza e del diritto alla protezione dei dati personali sono fatte risalire alla sezione 8, come nel caso della sentenza che qui si commenta. In particolare, la Corte Suprema ha ritenuto che tale sezione protegga le persone e non i luoghi[23] e, anzi, si estende alla protezione delle informazioni personali[24]. 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[25]. In sostanza si applicherà la sezione 8 quando la privacy sia invasa da un « search or sei-

(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.

[19] 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. Nella sentenza in commento non si affronta questa problematica, in quanto era stata la stessa Corona che nei gradi di giudizio inferiori ad ammettere questa applicabilità (cf. par. 38 della sentenza).

Si deve chiarire che, sebbene la Carta non trovi applicazione nei rapporti fra privati, la Suprema Corte ha affermato a più riprese che le corti dovrebbero incorporare i valori della Carta nelle proprie interpretazioni inerenti la privacy fra privati (v. *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).

[20] 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*, in 41 *Case W. Res. L. Rev.* 831 (1991), che discute circa l'opportunità di tale eventuale modifica costituzionale.

[21] 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. Si vedano inoltre le altre opere a commento della *Charter* citate.

[22] V. ad es. *R. v. O'Connor*, [1995] 4 S.C.R. 411; *M. (A.) v. Ryan*, [1997] 1. S.C.R. 157.

[23] 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*, 389 U.S. 347 (1967), di interpretazione del Quarto Emendamento della Costituzione americana, con contenuto molto simile alla Sezione 8 della *Canadian Charter of Rights and Freedoms*.

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

[25] *R. v. Plant*, cit., par. 26.

zure », mentre si applicherà la sezione 7 come protezione costituzionale al di fuori di tali ipotesi[26].

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[27]. Ci sono inoltre due barometri con cui tarare 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[28]. Per quanto più in particolare riguarda quest'ultimo aspetto, l'esistenza e la profondità di una aspettativa di privacy devono essere decise caso per caso[29].

In un caso per molti versi analogo a quello qui esaminato[30], la decisione della Corte d'Appello dell'Alberta andò in diversa direzione rispetto alla sentenza della Corte Suprema: durante attività di manutenzione di una casella di posta elettronica di un proprio cliente, un *Internet service provider* (ISP) trovò degli allegati contenenti foto pedo-pornografiche. Quindi informò la polizia, consegnando copia delle *e-mail* con allegati. Durante il processo, la difesa dell'imputato sostenne che vi fosse stata una violazione della privacy sulle *e-mail* e quindi una violazione dei diritti protetti dalla *Charter of Rights and Freedoms*. La Corte ritenne che, pur avendo l'uomo una ragionevole aspettativa di privacy, essa non avesse la stessa gradazione della privacy che invece ci si attende nella posta « fisica ». Conseguentemente, l'ispezione effettuata dall'ISP e dalla polizia sul computer dell'imputato, doveva considerarsi lecita e legittima[31].

Passando ad analizzare alcuni casi insorti nel contesto lavorativo, vale la pena di soffermarsi principalmente sui casi in stretta relazione con la sentenza qui esaminata, ovverosia le fattispecie di controllo delle *e-mail* e delle informazioni dei lavoratori contenute in computer di lavoro[32].

---

[26] Mcisaac et al., *The law of privacy in Canada*, cit., 2-9.

[27] 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.

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

[29] 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, citata anche dalla sentenza qui esaminata ai par. 40 ss, che a sua volta applica un test cosiddetto della « totalità delle circostanze ».

[30] *R. v. Weir* (1998), 59 Alta. L.R. (3d) 319 (Q.B.).

[31] *R. v. Weir* (1998), cit., par. 56-77, *passim*.

[32] 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?*, in 20 *Advocacy Quarterly* 221 (1998).

Altra fattispecie spesso affrontata nelle decisioni giurisprudenziali è quella della videosorveglianza dei lavoratori. Nella maggioranza di queste decisioni si registra il riconoscimento di un diritto alla privacy del lavoratore, da valutarsi secondo ciò che è « ragionevole nelle circostanze » (cfr. *Re Doman Forest Products Ltd*, 13 L.A.C. (4th) 275, par. 279 ss. V. inoltre *St. Mary's Hospital and H.E.U*, 64 L.A.C. (4th) 382, decisione arbitrale del 1997 adottata in British Columbia; *Re Toronto Transit Commission and A.T.U., Loc. 113 (Belsito)*, 95 L.A.C. (4th) 402. de-

Nel 1999 la Corte Suprema del British Columbia decise il caso *Pacific Northwest Herb Corp. v. Thompson*[33]. 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 ad 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[34].

Nel caso *Briar v. Canada (Treasury Board)* del 2003[35], 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. Successiva-

cisione arbitrarle dell'Ontario del 1999; *New Flyer Industries Ltd. and C.A.W. - Canada, Loc. 3003 (Mogg)*, 85 L.A.C. (4th) 304 decisione arbitrale del 2000 in Manitoba). Secondo M. Geist, *Computer and E-Mail Workplace Surveillance In Canada*, cit., 31 e ss., i casi più risalenti si concentravano principalmente sull'aspettativa di privacy del lavoratore, mentre attualmente pare registrarsi una tendenza a valutare la ragionevolezza della sorveglianza in sé. Si v. anche, in senso critico rispetto all'approccio da ultimo citato: A. Levin, *Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada*, cit., 220 ss. La giurisprudenza delle corti del Québec risulta la più chiara e precisa, in quanto ha sviluppato dei test da applicarsi ai casi concreti al fine di valutare la ragionevolezza della sorveglianza effettuata dai datori di lavoro, v. ad es. *Le Syndicat des Travailleurs(euses) de Bridgestone-Firestone de Joliette (CSN) v. Me Gilles Trudeau et Bridgestone/Firestone Canada inc.*, [1999] R.J.D.T. 1075, par. 72. Più di recente si assiste al fenomeno dell'utilizzo della biometrica da parte dei datori di lavoro. Si vedano le decisioni arbitrali: *Cascadia Terminal and G.W.U., Loc. 333 (Re)*, (2004) 123 L.A.C. (4th) 203 e *Canada Safeway Ltd. and United Food and Commercial Workers Union*, Local 401 (2005) relative a meccanismi di scansione delle impronte digitali per il controllo degli orari in entrata e in uscita, quest'ultima riformata da *IKO Industries Ltd. v. U.S.W.A.*, Local 8580, 2006 CarswellOnt 7541 (Ont. S.C.J.), nonché *Agropur (Natrel) v. Milk and Bread Drivers, Dairy Employees, Caterers and Allied Employees (Teamsters Local Union No. 647)*, 2008 CanLII 66624 (ON LA). V. inoltre il PIPEDA Case Summary #281 relativo al riconoscimento vocale dei lavoratori necessario per accedere al sistema informatico aziendale. Si veda per un approfondimento: G.T. Clark, *Biometrics in the Workplace: Where to Draw the Line?*, 2006, reperibile all'url: *http://www.governmentevents.ca/pipa2006/presentations/a1_gary_clarke_-paper.pdf*.

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

[34] *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*.

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

mente 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[36].

Altro caso simile, citato anche in *Briar v. Canada*, fu deciso nel 1999 in sede arbitrale[37]: un dipendente era stato licenziato per aver scritto un'*e-mail* fortemente critica nei confronti del datore di lavoro e dei colleghi ad 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[38]. Questi due elementi convinsero l'arbitro che non vi poteva essere una legittima aspettativa di privacy[39].

In uno dei pochissimi casi in cui il giudicante dovette considerare la richiesta di sopprimere delle prove relative a posta elettronica in base a una questione di privacy, l'arbitro ritenne che quando non vi sia una *policy* specifica, un dipendente non possa avere una legittima aspettativa di privacy rispetto ad *e-mail* ricevute e spedite sul posto lavoro, attraverso gli strumenti datoriali nell'orario lavorativo[40]. 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[41].

Quanto detto fa in realtà riferimento solo ad ipotesi in cui non esista uno « statutory privacy right ». Invero, come più sopra accennato, le nor-

---

[36] *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).

[37] *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.

[38] 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.

[39] *Camosun College v. C.U.P.E., Local 2081*, cit., par. 21.

[40] *Milsom v. Corporate Computers Inc.*, [2003] A.J. No. 516 - Atla. Q.B.), par. 41.

[41] *Poliquin v. Devon Canada Corporation*, 2009 ABCA 216.

mative canadesi in tema di privacy proteggono tutte le informazioni personali[42].

Pochissime le decisioni di senso opposto a quelle finora riassunte. Fra queste, una decisione arbitrale che ha ritenuto che il diritto del datore di ispezionare i contenuti del computer di un dipendente debba essere bilanciato con l'aspettativa di privacy del lavoratore e sia soggetto ad un test di ragionevolezza[43].

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[44]. Questo scenario sembra destinato a mutare con l'emanazione della sentenza in commento.

3. La decisione.

La sentenza che qui si commenta si pone in contrasto con le decisioni illustrate nel paragrafo che precede[45].

Il caso sottoposto all'esame della Corte Suprema scaturiva dal ritrovamento sul disco fisso di un computer « di lavoro » utilizzato da un dipendente di immagini pedopornografiche. In particolare, l'imputato — Richard Cole — insegnante di scuola superiore, era affidato un computer per ragioni lavorative, pur potendo egli utilizzare lo stesso saltuariamente anche per scopi personali. Durante lo svolgimento di attività di manutenzione, un tecnico aveva trovato sul pc portatile dell'imputato una cartella di file nascosta, contenente fotografie di una studentessa minorenne nuda e 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 esamina il contenuto e creò una « copia esatta » dell'*hard disc* per scopi investigativi.

Il giudice di primo grado (*trial judge*) escluse dalle prove tutto il materiale contenuto nel computer in quanto ottenuto in violazione della sezione 8 e 24(2) della *Canadian Charter of Rights and Freedoms*. La corte del *summary conviction appeal* rovesciò la decisione, ritenendo che non vi

---

[42] D. Michaluk, *Employer Access to Employee E-mails in Canada*, in 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.

[43] *Lethbridge College and Lethbridge College Faculty Assn. - Bird Grievance) - Re)*, [2007] A.G.A.A. No. 67, par. 31.

[44] D. Michaluk, *Employer Access to Employee E-mails in Canada*, cit., 95 e casi ivi citati alla n. 18. Statuizioni in senso contrario si possono leggere 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.

[45] Deve innanzitutto chiarirsi che si trattava di procedimento penale e non, come invece nelle decisioni arbitrali, di procedimento disciplinare.

fosse violazione di tale sezione. La Corte d'Appello dell'Ontario disattese quest'ultima decisione ed escluse il disco contenente i *file* temporanei di Internet, il pc portatile e la copia esatta dell'*hard disc*. Ritenne invece il disco contenente le fotografie della studentessa copiato dal tecnico fosse stato ottenuto in modo lecito e fosse pertanto ammissibile. Infine, dato che il *trial judge* aveva escluso erroneamente questa prova, la Corte d'Appello ordinò che fosse esperito un nuovo processo. Tale decisione era impugnata davanti la Suprema Corte, che sanciva con la sentenza in esame la violazione della sezione 8 ed ammetteva tuttavia con opinione di maggioranza le prove, in quanto rispettose della previsione di cui alla sezione 24(2)[46].

La Corte Suprema prende le mosse dal *leading case R. v. Morelli*[47] per concludere ritenendo che, per quanto affievolita, l'aspettativa di privacy del signor Cole doveva ritenersi esistente.

Nel procedimento penale *R. v. Morelli* la Corte Suprema elaborò un test per determinare quando un « search and seizure » (ispezione e sequestro) possa essere considerato ragionevole limitazione della privacy[48]. Come nella sentenza qui in commento, l'imputato chiedeva l'espunzione di alcune prove ottenute in violazione della Sezione 8 della Carta, secondo quanto disposto dalla Sezione 24(2)[49]. Fra le questioni da valutare v'era anche l'impatto della violazione dell'interesse alla privacy dell'accusato, in merito alla quale la corte sostenne che « è difficile immaginare un'invasione della privacy maggiore di quella derivante dall'ispezione di un com-

[46] Sebbene questo profilo della sentenza non sarà qui trattato, deve essere chiarito che l'ammissibilità delle prove era valutata alla luce della sezione 24(2) della *Canadian Charter of Rights and Freedoms*, titolata « Esclusione di prove che comportino discredito per l'amministrazione della giustizia » e che recita: « quando, in procedimenti [che riguardino la violazione di un diritto protetto dalla Carta], una corte concluda che le prove furono ottenute in maniera da violare o negare un diritto o una libertà garantita da questa Carta, le prove devono essere escluse se si stabilisca che, avendo riguardo a tutte le circostanze, l'ammissione di tali prove nel processo porterebbe discredito all'amministrazione della giustizia ». Ritenne la Corte che la condotta dell'ufficiale di polizia non fosse stata una violazione eccessiva della Carta. L'esclusione del materiale avrebbe avuto un impatto negativo nella funzione di ricerca della verità del processo penale, mentre l'ammissione dello stesso non avrebbe portato discredito per l'amministrazione della giustizia. Per questi motivi la Suprema Corte considerò le prove ammissibili. Di diversa opinione Justice Abella, per cui v. par. 107-136 della decisione qui commentata. Per un'analisi della sezione 24 della carta, v. R.J. Sharpe, K. Roach, *The Charter of Rights and Freedoms*, Toronto, 2009, 299 ss. G.A. Beaudoin, E. Mendes, *Canadian Charter of Rights and Freedoms - Charte canadienne des droits et libertés*, Markham, 2005, 1323 ss; più in particolare per la relazione fra sezione 8 e sezione 24(2) v. *Ibidem*, 699 ss.

[47] *R. v. Morelli*, 2010 SCC 8.

[48] 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, fra i siti preferiti, 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 incremento quando, dovendo tornare 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. Pertanto decise di denunciare 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.

[49] Sostanzialmente, per ottenere un mandato per poter ispezionare l'appartamento di Morelli, la polizia aveva fornito informazioni « selezionate » al Giudice di pace, la cui percezione della situazione era quindi stata falsata.

puter personale. I computer spesso contengono le nostre comunicazioni più intime. Contengono dettagli delle nostre situazioni finanziarie, mediche e personali. Essi rivelano perfino nello specifico i nostri interessi, preferenze e propensioni [...] Pertanto è difficile concepire una violazione della Sezione 8 con un impatto maggiore sull'interesse alla privacy protetto dalla Carta »[50].

Partendo da queste considerazioni, la *Supreme Court* ha ritenuto che, sebbene le regole interne all'istituto dove il signor Cole lavorava potessero diminuire la sua aspettativa di privacy, tale aspettativa per quanto diminuita, soprattutto se confrontata con l'aspettativa dell'imputato in *R. v. Morelli*, doveva comunque considerarsi *un'aspettativa*.

Quando esiste quest'aspettativa è necessario che vi sia un mandato basato su una legge che autorizzi la polizia alle perquisizioni. Mentre il preside aveva l'autorità per requisire ed ispezionare il computer, la polizia non aveva la stessa prerogativa e necessitava, invece, di un mandato. Il consenso del consiglio di istituto alle perquisizioni non aveva alcuna validità in quanto consenso del « terzo ». Quindi v'era differenza fra le copie create dai tecnici dell'istituto e quelle create dalla polizia: è su queste infatti che si poneva la questione di ammissibilità.

Come la corte stessa ha chiarito, 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[51].

Al fine di determinare se l'aspettativa dell'imputato fosse o meno ragionevole, la corte canadese ha applicato il cosiddetto « *totality of the circumstances test* »[52]. Esso si basa su quattro punti:

1) valutare il materiale esaminato dall'ispezione: considerato che si trattava di informazioni contenute nel disco fisso del computer e di file Internet, ciò 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[53];

2) valutare la possibilità di un interesse diretto nel materiale da parte del ricorrente: 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;

3) indagare circa l'eventuale aspettativa soggettiva di privacy dello stesso ricorrente: ciò era implicito e derivava direttamente da quanto nel punto 2. Restava da valutare il quarto punto;

4) giudicare se l'aspettativa fosse oggettivamente ragionevole, avendo avuto riguardo, appunto, alla totalità delle circostanze: con riguardo a questo, la Corte Suprema chiarisce subito che più il materiale oggetto di ispezione è vicino al nucleo intimo delle informazioni personali, più ciò inciderà sulla ragionevolezza dell'aspettativa di privacy. L'aspettativa

---

[50] *R. v. Morelli*, cit., par. 105-106.

[51] *R. v. Cole*, cit., par. 34-35.

[52] *R. v. Cole*, cit., par. 39 ss. Tale test fu formulato nella decisione *R. v. Edwards*, [1996] 1 S.C.R. 128 (S.C.C.).

[53] La corte canadese cita testualmente A. Westin, *Privacy and Freedom*, New York, 1967, 7.

di privacy deve essere valutata alla luce di ciò che altri soggetti, trovandosi nella medesima posizione, riterrebbero ragionevole.

Come accennato, la Corte confronta il caso *Cole* con il caso *Morelli*: in entrambi, infatti, entravano in gioco informazioni rilevatrici di aspetti molto personali dell'imputato, indice di un'alta aspettativa di privacy. Tuttavia, mentre in *Morelli* il computer era all'interno di un domicilio privato, in questo caso si trattava di un computer di lavoro, per cui si rendeva necessario valutare la realtà operativa del luogo di lavoro dell'imputato. Tale valutazione andava sia 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 che la tecnologia privavano l'imputato del controllo e dell'accesso esclusivi alle informazioni contenute nel *pc*)[54].

Quindi, sommando la totalità delle circostanze si ha, da un lato, che la natura delle informazioni in gioco e l'utilizzo personale del computer spingono 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, spingono nel senso contrario. Ciò tuttavia non era sufficiente, a parere della *Supreme Court*, ad eliminare totalmente l'aspettativa di privacy dell'accusato.

Ciò premesso, l'ispezione effettuata dalla polizia doveva considerarsi illecita in quanto effettuata senza mandato, o altra autorizzazione. Né valeva l'obiezione sollevata dalla Corona che sosteneva l'intervenuto consenso del terzo[55]. Ciò infatti significherebbe che un soggetto terzo possa rinunciare alla privacy altrui, facendo venire meno le garanzie previste dalla sezione 8 della *Charter*[56]. Questa teoria andrebbe a scontrarsi con i principi cardine della privacy nel sistema canadese, fra cui appunto spicca il consenso dell'interessato: consenso che dev'essere informato e liberamente dato.

Il consenso del soggetto interessato è infatti il più importante, anche se altamente controverso[57], dei principi su cui si basa l'intero impianto normativo canadese in tema di privacy, *in primis* del PIPEDA. Secondo il PIPEDA il consenso fornito dall'interessato è richiesto ogniqualvolta l'informazione è trattata da un terzo. Il consenso, che può essere ritirato in ogni momento[58], deve essere informato. Ciò significa che deve essere accompagnato da notizie circa gli scopi per cui i dati vengono raccolti ed utilizzati, fornite in modo che normalmente una persona possa compren-

[54] *R. v. Cole*, cit., par. 49-54.

[55] 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)). In particolare, la sentenza *Matlock* si basava sull'idea che il consenso del terzo potesse giustificarsi sul fatto che il soggetto interessato aveva assunto volontariamente il rischio che le informazioni a lui inerenti potessero incappare nell'applicazione del diritto. Tuttavia la Corte Suprema canadese aveva già rigettato in passato questo approccio, 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.).

[56] *R. v. Cole*, cit., par. 73-74.

[57] Si veda ad es. L.M. Austin, *Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda*, in 56 *University of Toronto Law Journal* 181 (2006).

[58] S. Perrin et Al., *The Personal Information Protection and Electronic Documents Act*, cit., 22 ss.

derli. Vi sono poi situazioni in cui il consenso non deve essere fornito perché inappropriato perché presunto[59].

Nonostante tali eccezioni, la Corte Suprema sottolinea come la teoria del consenso del terzo sarebbe incoerente anche con la giurisprudenza della corte stessa, in quanto si tratterebbe di consenso non volontariamente fornito, né fondato su sufficienti informazioni necessarie al fine di una scelta consapevole[60].

La sentenza in commento, dunque, si pone in contrasto con l'orientamento prevalente riassunto nel paragrafo precedente. Se infatti nella maggioranza delle decisioni l'aspettativa di privacy del dipendente sul luogo di lavoro si affievolisce a tal punto da scomparire, nella decisione *R. v. Cole*, le *policy* aziendali che permettono l'uso personale di strumenti di lavoro, quali il computer, assumono una rilevanza tale da fungere da fonte di aspettativa della *privacy*.

4. Cenni comparatistici: la situazione negli Stati Uniti.

Sebbene molto vicini in termini geografici, il Canada e gli Stati Uniti si trovano su posizioni piuttosto distanti per quanto riguarda il tema della privacy.

Invero, nel Paese dove il concetto stesso di privacy sembra essere nato[61], la disciplina del diritto alla riservatezza si presenta frammentaria e disomogenea, minandone in questo modo la tutela. La tutela della privacy è infatti affidata ad un alto numero di normative, le quali per lo più si concentrano su determinati settori e/o rispondono ad esigenze che si potrebbero definire « emergenziali »[62]. Il più importante fra questi interventi è probabilmente il Privacy Act del 1974, che fornisce ai cittadini alcuni diritti sulle informazioni che li riguardano che siano contenute in database governativi, compreso il diritto di visionare le informazioni e chiederne la modifica. Ogni divulgazione delle informazioni è soggetta al consenso dell'interessato, nonostante vi siano numerose eccezioni[63]. Questo *Act* non si applica ai privati o alle organizzazioni econo-

[59] Si veda, per la non appropriatezza consenso PIPEDA, Schedule 1, 4.3, Principle 3 - « Consent »; per la presunzione del consenso, PIPEDA, sezioni 7(1)-(3).

[60] *R. v. Cole*, cit., par. 77-78.

[61] L'immancabile citazione si riferisce a S.D. Warren, L.D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

[62] Le normative fanno riferimento ad esempio alla privacy « finanziaria » (Right to Financial Privacy Act - 1978), a quella delle comunicazioni elettroniche (Electronic Communications Privacy Act - 1986), alla privacy degli utenti telefonici 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). Rientra invece, a titolo d'esempio, negli interventi normativi di tipo emergenziale il Privacy Act del 1974, in risposta al c.d. « Scandalo Watergate », v. D.J. Solove, P.M. Schwartz, *Information Privacy Law*, New York, 2011, 701; e, per altri testi normativi, M.A. Sherman, *Webmail At Work: The Case For Protection Against Employer Monitoring*, 2007, 20-21, reperibile all'url: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=978075*.

[63] La più ampia di queste eccezioni è quella del cosiddetto « uso routinario » secondo cui quando un nuovo utilizzo sia compatibile con gli scopi per cui inizialmente l'agenzia ha raccolto di dati, l'informazione può essere divulgata ad altra agenzia senza il consenso dell'interessato (cf. Cf. 5 U.S.C. § 552a(b)(3)).

miche, ma soltanto alle agenzie pubbliche e, più precisamente, solo a quelle federali[64].

A fianco di queste normative si pongono alcune figure di *torts*[65], le regolamentazioni statati[66], e una protezione più ampia ricondotta alla Costituzione. Le regolamentazioni statali sono a loro volta settoriali, anche se rivolte sia al contesto pubblico sia a quello privato[67] e sebbene siano stati effettuati interventi specifici a tutela della privacy del lavoratore da parte di alcuni stati[68].

Per quanto riguarda la protezione costituzionale a livello federale, proprio come nel contesto canadese, seppur non esista una previsione che esplicitamente tuteli la privacy, essa è considerata protetta da più emendamenti[69].

Rileva principalmente per il presente scritto la protezione accordata dal Quarto Emendamento: « The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated [...] ». In *Olmstead v. United States*, attraverso una *dissenting opinion*, Justice Braindeis ritenne che tale 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[70]. Tale opinione dissenziente fu di assoluta importanza nella stesura della celeberrima sentenza *Katz v. United States*, in cui la *Supreme Court* ritenne che il Quarto Emendamento protegga le persone e non i luoghi[71]. Inoltre, nell'opinione concorrente di Justice Harlan fu delineato il cosiddetto « reasonable expectation of privacy » test, che permette di comprendere se la tutela prevista dal Quarto Emendamento possa essere accordata nel caso specifico. Il test prevede due fasi: nella prima si deve comprendere se il soggetto avesse un'aspettativa attuale soggettiva di privacy;

---

[64] D.J. Solove, P.M. Schwartz P.M., *Privacy, Information, and Technology*, New York, 2009, 304; D.J. Solove, P.M. Schwartz, *Information Privacy Law*, cit., 701 ss.

[65] 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*, in 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., 32-33.

[66] Ciascuno stato ha promulgato leggi di protezione della privacy sotto diversi profili, sia nel settore privato che pubblico. Solo alcuni, tuttavia, hanno emanato una legge generale che somigli al Privacy Act. Cf. D.J. Solove, P.M. Schwartz, *Information Privacy Law*, cit., 39; A.R. Levinson, *Workplace Privacy and Monitoring: The Quest for Balanced Interest*, in 59 *Cleveland State Law Review* (2011), 14 ss., disponibile all'url: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893706*.

[67] D.J. Solove, P.M. Schwartz, *Information Privacy Law*, cit., 39.

[68] Tutti adottati nel 2007: 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.

[69] 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.

[70] *Olmstead v. United States*, 277 U.S. 438 (1928), 478.

[71] *Katz v. United States*, 389 U.S. 347 (1967), 351.

nella seconda se tale aspettativa possa essere considerata dalla società come ragionevole[72].

Già nel 1965, tuttavia, 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[73]. Qualche anno più tardi la stessa corte ammise la protezione anche dell'aspetto informazionale della privacy, riconoscendo un interesse individuale ad evitare la divulgazione di fatti personali[74].

Passiamo ora ad analizzare situazioni più vicine a quella della sentenza canadese, che ricadono appunto sotto la copertura del Quarto Emendamento, la quale si avvicina molto alla Sezione 8 della carta costituzionale del Canada. Guardando ad alcuni casi risolti alle corti statunitensi, tuttavia, ci si accorge che in questo sistema il *search and seizure* dei computer non subisce particolari limitazioni. Ed anzi: in un caso in cui l'FBI si trovò a copiare il contenuto di un computer sito in Russia, la Corte del Western District di Washingon ritenne che non si trattasse di un sequestro secondo il Quarto Emendamento, perché non vi era interferenza con l'interesse dell'imputato o di un terzo nel possesso dei dati[75].

Simile a *R. v. Cole* che qui si commenta, *United States v. Andrus* è un caso in cui la polizia federale ottenne il consenso del padre di un uomo al fine di ispezionare il pc di quest'ultimo all'interno delle mura della casa di famiglia[76]. L'uomo era sospettato di aver scaricato sul proprio computer

---

[72] Cf. *Katz v. United States*, cit., 361. Questo tipo di test ha sollevato numerose problematiche, si veda ad es. R.G. Wilkins, *Defining the « Reasonable Expectation of Privacy »: An Emerging Tripartite Analysis*, in 40 *Vand. L. Rev.* 1077, 1089 (1987); G.A. Ashdown, *Legitimate Expectation of Privacy*, in 34 *Vand. L. Rev.* 1289 (1981); A. Libeu, *What is a reasonable expectation of privacy?*, in 12 *W. St. U. L. Rev.* 849 (1985). Si veda inoltre D.J. Solove, P.M. Schwartz, *Privacy, Information, and Technology*, cit., 99 ss. 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, inerente la circolarità dei requisiti del test.

[73] *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).

[74] *WhaleWhalen v. Roe*, 429 U.S. 589 (1977), 599. Il caso riguardava informazioni relative alla prescrizione di medicinali, che i medici dovevano per legge trasmettere al Dipartimento di Stato, che li avrebbe conservati nei propri database. Alcuni pazienti e medici, insieme ad associazioni di categoria, impugnarono questa legge. Sebbene la Corte Suprema non la abrogò, ritenne che esistesse un diritto alla protezione dei dati personali, sulla base di due diversi interessi: il primo teso ad evitare la diffusione di informazioni personali e il secondo relativo alla necessità di indipendenza nel compiere decisioni di rilievo.

[75] *United States v. Gorshkov*, 2001 U.S. Dist. LEXIS 26306, 8. Appare evidente la differenza di trattamento che si sarebbe avuta se il fosse stato il computer inteso come « oggetto fisico » a subire il sequestro e non invece i dati, come nel caso concreto (sulle differenze fra ispezioni effettuate in un appartamento e ispezioni effettuate su di un computer v. O.S. Kerr, Searches and Seizuers in a Digital Works, 119 Harvard Law Review 531, 536 ss (2005). Sarebbe peraltro bastato paragonare le informazioni all'interno del computer al contenuto di una conversazione privata secondo S.W. Brenner, B.A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, in 8 *Mich. Telecomm. & Tech. Law Review* 39, 111-112 (2002), nonché 106 ss. per ulteriori spunti sull'attività di copiatura di informazioni personali da un computer.

[76] *United States v. Andrus*, 483 F.3d 711 (10th Cir. 2007).

immagini pedopornografiche. Nella sentenza si chiarisce specificatamente che, pur non essendo permesso effettuare perquisizioni senza mandato, il consenso alla perquisizione è valida eccezione. Al consenso del soggetto interessato equivale il consenso del terzo che abbia autorità sulla cosa soggetta ad ispezione, sia che il consenso del terzo sia effettivo sia che sia apparente[77]. In tal caso la Corte ritenne che, sebbene vi fosse una *password* a protezione del computer e in verità il padre non avesse nessun controllo né accesso allo stesso, la polizia aveva correttamente effettuato l'ispezione sulla presunzione che, permettendo il padre la perquisizione della casa ed essendovi un solo computer, egli fosse un utilizzatore, anche se solo parziale, del pc. Per comprendere se l'ispezione rimanesse dentro ai confini del consenso prestato dal padre, i giudicanti applicarono, come nel caso canadese, il test della « totalità delle circostanze »[78]: la situazione, così come si presentava agli occhi degli ufficiali di polizia, dava adito a ritenere che il padre fosse un utilizzatore del computer e pertanto avesse l'autorità di prestare il consenso all'ispezione del computer, sebbene contenesse informazioni di un terzo, ossia del figlio, che erano proprio quelle cercate dalla polizia[79].

Venendo ora alla privacy di cui gode il lavoratore, si deve premettere che i lavoratori pubblici sono protetti da una serie di interventi legislativi, dal *Privacy Act* alle normative sulle intercettazioni[80], nonché dal Quarto Emendamento, anche se limitatamente. Vi sono poi molte costituzioni statali che proteggono la riservatezza dei dipendenti pubblici ed inoltre i dipendenti possono far leva su alcune figure di *tort* a protezione della privacy, soprattutto sul *tort* di « intrusion upon seclusion »[81]. 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 vi si applica la gran parte delle costituzioni statali[82]. Sono invece applicabili alcuni *Act* in tema di privacy e[83], inoltre, talvolta ai lavoratori sono concessi specifici rimedi contrat-

[77] *United States v. Andrus*, cit., 716. L'effettiva autorità si ha quanto vi sia o l'uso e l'accesso condiviso dell'oggetto di proprietà oppure il controllo della cosa per la maggioranza degli scopi, v. *Ibidem*. La stessa sentenza fornisce gli indici per classificare un « personal computer » ai fini del Quarto Emendamento, v. *Ibidem*, 718 ss. La stessa sentenza che qui si commenta menziona il « third party consent » come dottrina accettata ed applicata negli Stati Uniti, cf. *R. v. Cole*, cit., par. 75-76.

[78] Citando *United States v. Pena*, 920 F.2d 1509, 1514 (10th Cir. 1990).

[79] *United States v. Andrus*, cit., 720 ss.

[80] D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information privacy law*, New York, 2006, 800; 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.

[81] S. Diluzio, *Workplace E-Mail: It's Not As Private As You Might Think*, 25 Delaware Journal Of Corporate Law 741 (2000), 749-750.

[82] 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), par. 842).

[83] 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*, cit., 4 ss.

tuali[84]. La frammentazione e la lacunosità della normativa sono fra i sintomi di un sistema dove il mercato del lavoro è lasciato libero di agire, secondo il principio per cui le parti dovrebbero essere libere di contrattare a loro piacimento[85].

Come nel contesto canadese, anche negli Stati Uniti il concetto di *reasonable expectation of privacy* è stato vagliato alla luce delle nuove tecnologie. Questa ragionevolezza, oltre ad essere necessaria per determinare l'applicabilità del Quarto Emendamento, si pone quale requisito anche per i casi di *tort of intrusion upon seclusion*: sarà illecita quell'intrusione nell'aspettativa di privacy che sia altamente offensiva[86].

Con una sentenza del 1997, la District Court della Pennsylvania ritenne che l'utilizzo delle *e-mail* del sistema aziendale non potesse generare una ragionevole aspettativa di privacy. Inoltre, anche qualora si fosse voluto ritenere esistente questa aspettativa, la sua violazione non appariva alla corte considerevole e altamente offensiva. In ogni caso, l'interesse della società datrice di lavoro a prevenire la circolazione di commenti inappropriati e non professionali o addirittura attività illegali effettuate attraverso il suo sistema di comunicazione ha più importanza di qualunque interesse alla privacy possa avere il dipendente in tali comunicazioni[87].

Il caso *City of Ontario v. Quon* riguardava il dipartimento della polizia che aveva installato una rete *wireless*, utilizzabile dai lavoratori mediante i cercapersone. La *policy* del dipartimento non ammetteva l'utilizzo di questa rete per benefici personali e il dipartimento si riservava il diritto di monitorare le attività della rete. Uno dei dipendenti sforò più volte il limite massimo di messaggi inviabili, finché il dipartimento richiese ed ottenne dalla società gestrice della rete le trascrizioni dei contenuti di tali

---

[84] D.J. Solove, M. Rotenberg, P.M. Schwartz, *Information privacy law*, cit., 800; D.J. Solove, P.M. Schwartz, *Privacy, Information, and Technology*, cit., 988.

[85] J.D.R. Craig, *Privacy and Employment Law*, cit., 58.

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

[87] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), 101. 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), ritenendo che colui che trasmette una *e-mail* ha 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?*, in 60 *U. Toronto Fac. L. Rev.* 85 (2002), 90 ss. Per dei commenti sulle prime decisioni inerenti il controllo della posta elettronica dei dipendenti v. P.F. Gerhart, *Employee Privacy Rights In The United States*, in 17 *Comp. Lab. L.J.* 175 (1995), spec. 199 ss.; P.E. Hash, C.M. Ibrahim, *E-Mail, Electronic Monitoring, And Employee Privacy*, in 37 *S. Tex. L. Rev.* 893 (1996).

messaggi, che si rivelarono avere contenuto personale e a sfondo sessuale. Il dipendente citò sia il dipartimento che la società gestrice della rete, sostenendo una violazione del Quarto Emendamento[88]. La corte d'appello si interrogò circa l'esistenza di una protezione da parte di tale emendamento sui messaggi scambiati dagli ufficiali[89]. 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 ad una aspettativa di privacy nei messaggi.

Il caso fu poi analizzato dalla Corte Suprema[90], che rovesciò la decisione della corte inferiore. Ritenne che la corte che, 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 esaminazione. 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[91].

Venendo infine alle ispezioni dei computer aziendali, in *Leventhal v. Knapek* l'attore, dipendente di un datore pubblico, lamentava che le ispezioni avvenute sul suo computer fossero state effettuate in violazione del Quarto Emendamento[92]. Considerate le circostanze, la corte ritenne che Leventhal avesse in effetti una ragionevole aspettativa di privacy, ma che essa dovesse essere bilanciata con l'interesse pubblico all'ispezione, che era indirizzata a comprendere se vi fossero delle condotte sconvenienti da parte del dipendente, tra cui l'utilizzo di *softwares* non autorizzati. L'interesse del lavoratore soccombette però contro quello pubblico, in quanto l'ispezione poteva considerarsi lecita e non eccessivamente intrusiva rispetto alla natura della condotta del dipendente[93].

Nel caso *United States v. Simons*[94], un dipendente del Foreign Bureaou of Information Services citò in giudizio l'amministrazione datrice di lavoro per un'ispezione sul suo computer che egli riteneva essere 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. Uno dei colleghi creò una copia del disco fisso ad insaputa di Simons, che fu successivamente imputato per detenzione di materiale pedopornografico. Ritenendo che l'ispezione avesse violato i suoi diritti del Quarto

[88] I ricorrenti ritenevano violato anche lo *Stored Communications Act*, 18 U.S.C. Capitolo 121, §§ 2701-2712.

[89] *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.

[90] *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

[91] *City of Ontario v. Quon*, cit., 2631-2632.

[92] *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001).

[93] *Leventhal v. Knapek*, cit., 75, facendo riferimento a *O'connor et al. v. Ortega*, 107 S. Ct. 1492 (1987), decisione sui diritti nascenti dal Quarto Emendamento per i dipendenti pubblici, con riguardo alle ispezioni amministrative sul luogo di lavoro effettuate dai superiori durante investigazioni relative alle violazioni delle *policy* aziendali, e non invece per casi di reato.

[94] *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).

Emendamento, il lavoratore richiese la soppressione delle prove ottenute mediante tale ispezione. Alla luce delle policy interne al FBIS che statuivano chiaramente la possibilità di controlli, ispezioni e monitoraggi, e che i dipendenti potevano utilizzare Internet solo per affari ufficiali governativi, la corte ritenne che non vi fosse aspettativa di privacy. Nonostante quanto ritenuto personalmente da Simons, la sua aspettativa di privacy non poteva ritenersi ragionevole. 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 in remoto[95].

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

Vale la pena infine di illustrare un ultimo caso, molto simile a *United States v. Simons*, ma che aveva come protagonisti un lavoratore ed un datore di lavoro del settore privato[96]. Il signor Ziegler era sospettato di detenere materiale pedopornografico, sospetto poi appurato da dei monitoraggi sul traffico Internet effettuato dal suo computer. Successivamente due colleghi di Ziegler fecero nottetempo due copie del disco rigido del computer. La compagnia datrice di lavoro consegnò poi una copia insieme con il computer di Ziegler all'FBI, i cui 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. Facendo riferimento al *leading case* Mancusi[97], la corte ritenne che Ziegler avesse un'aspettativa di privacy riguardo al suo ufficio, che tra il resto era tenuto chiuso a chiave. Quindi l'ispezione dell'ufficio effettuata dai suoi colleghi era indubbiamente da considerarsi quale ispezione, la stessa tuttavia era stata acconsentita dal datore di lavoro. Egli poteva validamente acconsentire all'ispezione, in quanto si tratta di cose di proprietà su cui il datore aveva un controllo e al cui contenuto, peraltro, il datore aveva possibilità di accesso. 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, quindi, Ziegler non poteva ragionevolmente attendersi che il suo computer non venisse ispezionato e, in ogni caso la società datrice aveva legittimamente acconsentito all'ispezione, per cui le prove ottenute mediante l'ispezione non dovevano essere soppresse[98].

---

[95] *United States v. Simons*, cit., 398-399; 401. Ancora una volta si fa riferimento a *O'connor et al. v. Ortega*, cit.

[96] *United States v. Ziegler*, 474 F. 3d 1184 (9th Cir. 2007).

[97] *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.

[98] *United States v. Ziegler*, cit., 1189-1193.

Si può notare dall'illustrazione che precede che le sentenze statunitensi sono tutte dello stesso segno[99]: raramente si possono riscontrare sentenze di diversa soluzione rispetto a quelle qui elencate, soprattutto per i lavoratori del settore pubblico che, pur avendo maggiori garanzie sulla carta, di fatto le hanno viste erodersi negli anni[100].

5. Riflessioni conclusive.

I sistemi canadesi e statunitense di protezione della privacy si differenziano molto non solo per il profilo legislativo, ma anche sul piano operazionale. Invero, nonostante vi siano degli aspetti in comune, quali le disposizioni costituzionali, le normative canadesi possono dirsi omnicomprensive, mentre gli interventi statunitensi sono per lo più settoriali.

Si è illustrato come entrambi i sistemi si basino sull'idea di « ragionevole aspettativa di privacy » applicando, in sostanza, *test* molto simili fra loro[101], al fine di determinare la tutelabilità della situazione concreta da parte di disposizioni costituzionali molto vicine fra loro quali il Quarto Emendamento statunitense e la Sezione 8 della *Charter* canadese.

Ciò nonostante, sul piano operativo, i due sistemi si trovano a raggiungere risultati differenti, e questo avviene sebbene le corti di entrambi i Paesi prestino attenzione alle policy aziendali. Per meglio dire: sebbene fino a non molto tempo fa le sentenze emesse in entrambi i Paesi in materia di privacy del lavoratore fossero del medesimo segno, ovvero tendenti a non riconoscere una privacy in capo al dipendente, di recente la tendenza in Canada va mutando. Segno indelebile di questo mutamento è proprio la sentenza che qui si commenta, che si pone come punto fermo e di svolta: nonostante le *policy* aziendali fossero chiare, nonostante la proprietà del *computer* fosse del datore di lavoro, nonostante il consenso fornito da quest'ultimo, l'aspettativa di privacy del dipendente non viene meno.

I rilievi effettuati dalla Corte Suprema canadese appaino lungimiranti anche rispetto a ciò che plausibilmente sarà il futuro: il *cloud*. Se infatti già fin d'ora non rileva la proprietà del computer né il consenso del datore di lavoro, a maggior ragione questi non rileveranno quando le informazioni personali del lavoratore saranno immagazzinate in *server* lontani, cui si può avere accesso da ogni punto del globo[102].

---

[99] 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*, 2012 U.S. Dist. LEXIS 90674 (E.D. Pa. 2012).

[100] V. sul punto D.C. Dammeir, *Fading Privacy Rights of Public Employees*, in 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*, in 7 *Computer L. Rev. & Tech. J.* 273 (2003), 285-286; 290 ss.

[101] Mi riferisco al test introdotto da Justice Harlan in *Katz v. United States* e a quello rinvenibile nel caso canadese *R. v. Plant* (quest'ultima fece invero riferimento a *Katz*).

[102] Su questo si veda la *dissenting opinion* di Justice Abella nella sentenza in commento, par. 107-109.

Fondamentale rimane, in ogni caso concreto, un effettivo bilanciamento degli interessi e dei diritti in gioco: effettivo nel senso che esso va concretamente effettuato e non solo formalmente enunciato. In tal senso le soluzioni canadesi sembrano confacersi di più ad un modello « caso per caso » rispetto a quelle statunitensi che poco spazio lasciano ai diritti del lavoratore.

Federica Giovanella