

ESTRATTO

# RIVISTA TICINESE DI DIRITTO

II- 2014

*Michele Albertini / Philippe Bolgiani / Giordano Costa*

## **Accessibilità ai messaggi di telefonia cellulare e protezione dei dati**

**Utilizzabilità, valore probatorio e ammissibilità  
ai fini processuali di SMS nell'ambito lavorativo  
pubblico e privato**

Direzione e responsabilità editoriale:

Prof. Dr. Marco Borghi  
e-mail: marco.borghi@unifr.ch

Redazione della parte fiscale:

Dr. Andrea Pedroli, Presidente della Camera di diritto tributario  
e-mail: andrea.pedroli@ti.ch

incaricati dal Consiglio di Stato

Edita da: Cancelleria dello Stato del Cantone Ticino e  
Helbing Lichtenhahn, Basilea (www.helbing.ch)

Distribuzione: – Ufficio della legislazione, delle pari opportunità e della trasparenza,  
6501 Bellinzona (e-mail: rtid@ti.ch)  
– Schweizer Buchzentrum, Industriestrasse Ost, 4614 Hägendorf

Coordinamento e allestimento: Gibi Borghi  
e-mail: gibi.borghi@unifr.ch

Stampa: Tipografia Mazzoni Moduli SA - 6595 Riazzino  
e-mail: mazzoni-moduli@ticino.com

Copertina: riproduzione da Cornelia Forster

ISSN 1661-0954 – ISBN 978-3-7190-3624-9 (Helbing Lichtenhahn)  
ISBN 978-88-6303-042-6 (Repubblica e Cantone Ticino)

# Accessibilità ai messaggi di telefonia cellulare e protezione dei dati

## Utilizzabilità, valore probatorio e ammissibilità ai fini processuali di SMS nell'ambito lavorativo pubblico e privato

*Michele Albertini\* / Philippe Bolgiani\*\* / Giordano Costa\*\*\**

1. Introduzione
2. Il caso
3. L'uso della telefonia cellulare nel contesto giuridico generale
4. Condizioni per l'accesso e l'analisi di messaggi di telefonia cellulare
5. Valore probatorio di messaggi di telefonia cellulare
6. Conclusioni

### **1. Introduzione**

Il tema dell'accessibilità e dell'utilizzabilità di messaggi di telefonia cellulare gestiti sulla telefonia mobile di servizio nell'ambito lavorativo non sembra – finora almeno e per quanto desumibile – essere stato oggetto di particolari approfondimenti dottrinali e giurisprudenziali, né di linee guida di autorità di protezione dei dati. Partendo da un caso illustrativo in parte realmente accaduto – e nell'intento di colmare, almeno parzialmente, questa lacuna – la presente analisi si concentra sugli elementi e sulle variabili generali, d'ordine tecnico, pratico e giuridico, con i quali il datore di lavoro e i suoi collaboratori possono essere confronta-

---

\* Dott. iur., incaricato cantonale della protezione dei dati e consulente giuridico del Gran Consiglio.

\*\* Dipl. ing. inf. ETHZ, consulente informatico presso l'Incaricato cantonale della protezione dei dati.

\*\*\* Lic. iur., giurista presso l'Incaricato cantonale della protezione dei dati.

ti. Dopo aver inquadrato l'uso della telefonia cellulare nel contesto giuridico generale, l'analisi si prefigge di individuare se e a quali condizioni legali il datore di lavoro possa acquisire legalmente dati inerenti alla messaggiera della telefonia mobile di servizio di un dipendente a rapporto di lavoro concluso, se questi dati siano ammissibili nell'ambito di eventuali procedure formali (come per esempio inchieste amministrative o disciplinari, oppure ancora in sede giudiziaria in caso di ricorso) e quale possa essere, oggettivamente, il loro valore probatorio.

## 2. Il caso

Concluso il suo rapporto di servizio, un funzionario ha riconsegnato il materiale di servizio, trattenendo per sé alcuni oggetti utilizzati che il datore di lavoro non era intenzionato a riprendere, lasciandone invece altri, dichiarando che di questi il datore di lavoro avrebbe potuto fare ciò che desiderava, quindi anche gettarli. Tra gli oggetti riconsegnati figurava anche un telefono mobile di servizio concessogli in uso. Nell'ambito dei lavori di riordino dell'armadio dell'ormai ex dipendente è stato rinvenuto un secondo telefono mobile di servizio, più vecchio, di cui a suo tempo egli aveva chiesto la sostituzione, poi avvenuta, ma che non era stato restituito. Nell'ambito delle verifiche sul suo buon funzionamento e sulle possibilità di riutilizzo di questo telefono, il servizio competente ha rilevato la presenza di messaggi di testo (SMS, acronimo dell'inglese *Short Message Service* o *Short Message System*) in entrata, li ha aperti e visionati, constatando un contenuto suscettibile di violare i doveri di servizio o addirittura norme penali. Il rinvenimento di questi messaggi provenienti da terzi – riconosciuti come dipendenti, rispettivamente ex dipendenti del medesimo ente pubblico in base ai numeri di telefono da cui sono stati spediti i messaggi – è stato segnalato al superiore, accompagnato da un loro tabulato su supporto cartaceo con i contenuti e i dati marginali (numero di telefono dei mittenti, data e ora degli invii).

### 3. L'uso della telefonia cellulare nel contesto giuridico generale

3.1. I servizi di telefonia vengono sempre più spesso, e negli ambiti più disparati (tra i quali l'impiego privato e pubblico), fruiti mediante l'uso di telefoni cellulari o terminali mobili. È un'evidenza certa, siccome tali dispositivi possono supportare, grazie all'evoluzione tecnologica recente e alla loro capillare diffusione, numerose funzionalità (non più semplicemente limitate al classico collegamento telefonico tra due utenti): possono cioè permettere anche di comunicare in conferenza e nella forma di videochiamate, di inviare e ricevere messaggi di diversa struttura (SMS, MMS, Email, Fax, ecc.), di ricevere e trasmettere, scaricare e caricare di dati di diversa natura, formato e in molte modalità tramite la rete Internet, di ricevere programmi radio e televisivi, di gestire molti tipi di applicativi e di *files* (audio, video, testo, ecc.) nei formati più diversi, di determinarne la localizzazione attraverso una rete satellitare, e così via.

3.2. A dipendenza dal modello, il telefono cellulare – la cui tipologia più evoluta, come lo *smartphone*, è completamente assimilabile a un personal computer – permette di elaborare svariate categorie di informazioni di natura personale quali, ad esempio, numeri telefonici dei mittenti e dei destinatari, indirizzi postali e di posta elettronica, messaggi di telefonia mobile e di posta elettronica e i loro dati marginali (quali la data e ora di invio e di ricezione, ecc.), agenda, fotografie, *files* audio e video, indirizzi e cache di Internet, profili di movimento tramite GPS, documenti e credenziali di accesso a tutti i servizi in rete (password) nonché, nei modelli più recenti, dati biometrici. Per quanto riguarda peculiarmente gli SMS – che configurano probabilmente la forma tecnicamente più semplice di comunicare, a fronte delle enormi possibilità offerte oggi dalla tecnologia – essi consistono in brevi messaggi in formato testo trasmessi da un telefono cellulare a (di regola) un altro. Nella memoria dei telefoni cellulari appare tradizionalmente il numero telefonico del mittente, sostituito visivamente – in caso di memorizzazione del numero nella rubrica telefonica – dal suo nome, come pure la data e l'ora di invio, rispettivamente di ricezione, a dipendenza delle impostazioni date al telefono.

Il fatto che questa forma comunicativa sia più semplice rispetto ad altre più moderne e complesse non deve tuttavia indurre a credere che essa sia, per certi versi, privilegiata. Il discorso va, anzi, posto su un altro piano: la tipologia di informazioni (tra cui gli SMS) elaborate in un telefono cellulare e il modo di elaborarle dipendono essenzialmente dal tipo di dispositivo impiegato, con le funzionalità che gli sono proprie. Nella vita quotidiana, che sia privata o professionale, i tipi di cellulare usati sono di categorie e di epoche diverse, tanto che molti modelli – per quanto attiene alle rispettive funzionalità – non sono neppure, di fatto, confrontabili, vista la loro varietà ed eterogeneità. Per poter valutare le potenzialità e le caratteristiche di un telefono cellulare quanto alla possibilità di impiegarlo per trasmettere o ricevere SMS, con le relative modalità, occorre quindi conoscerlo. E questo è un primo rilievo importante, che costituisce una vera e propria variabile.

3.3. Ad ogni buon conto – ed è un minimo comune denominatore di valenza generale che prescinde dal tipo di telefono cellulare – nella misura in cui si riferiscono a persone identificate o identificabili, le informazioni ivi contenute ed elaborate rappresentano *dati personali* ai sensi del diritto generale sulla protezione dei dati personali disciplinato a livello federale, nella legge federale sulla protezione dei dati (LPD<sup>1</sup>), e cantonale ticinese, nella legge sulla protezione dei dati personali (LPDP<sup>2</sup>). Se contengono dati relativi a opinioni o attività religiose, filosofiche o politiche, alla sfera intima, allo stato di salute o a possibili reati, alle relative pene inflitte e ai provvedimenti adottati, i dati in questione sono qualificati come meritevoli di particolare protezione (detti anche sensibili), ai sensi degli art. 3 lett. c LPD, rispettivamente 4 cpv. 2 LPDP, che sono come tali assoggettati a protezione accresciuta (in particolare, per quanto riguarda la loro acquisizione e trasmissione, e quindi il diritto di accedervi, nonché le misure di sicurezza). Questi dati, combinati fra loro, possono peraltro anche costituire un profilo della personalità, ovvero una compilazione di dati che permette di valutare caratteristiche essenziali della

---

<sup>1</sup> Legge del 19 giugno 1992 (RS 235.1).

<sup>2</sup> Legge del 9 marzo 1987 (RL 1.6.1.1).

personalità di una persona fisica (art. 3 lett. d LPD), che, sia nel diritto federale che nel diritto cantonale, sono considerati come dati sensibili.

I dati personali trattati nell'ambito della telefonia mobile possono quindi essere di diversa natura ed elaborati in modo molto variegato: solo dopo aver determinato questi elementi, applicati al dispositivo impiegato, è possibile, in un caso concreto, definire le esigenze legali per la loro elaborazione dal profilo della protezione dei dati. Questo al fine di prevenire una violazione della personalità e della sfera privata, che è lo scopo primario dell'impianto giuridico introdotto dalle citate leggi generali sulla protezione dei dati.

In un'ottica generale, i principi guida in materia disciplinati dalle normative indicate – validi indipendentemente dalla tecnologia impiegata, come pure dagli scopi, dai modi e dalle procedure utilizzate (art. 2 cpv. 1 LPDP) – sono essenzialmente i seguenti (art. 4 e 5 LPD, rispettivamente 6 e 7 LPDP). Anzitutto, un'elaborazione di dati personali deve essere lecita: ciò è il caso nella misura in cui essa si fonda su una base legale oppure se serve all'adempimento di un compito legale. Per quanto attiene ai dati personali meritevoli di particolare protezione, il diritto ticinese stabilisce che la loro elaborazione è lecita se lo prevede esplicitamente una legge o lo esige, in modo perentorio, l'adempimento di un compito legale, oppure la persona interessata vi ha acconsentito esplicitamente o il suo consenso può essere presunto siccome essa beneficia di prestazioni pubbliche. Il diritto della protezione dei dati prevede inoltre una serie di principi che l'organo responsabile di un'elaborazione di dati personali deve rispettare. In particolare, i dati personali elaborati devono essere idonei e necessari all'adempimento dei rispettivi compiti legali (principio della proporzionalità). Inoltre, i dati non possono essere utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente erano stati raccolti (principio della finalità), ritenuto che la raccolta e l'elaborazione di dati deve essere riconoscibile per la persona interessata (principio della trasparenza) e i dati devono essere esatti nonché, nella misura in cui lo scopo dell'elaborazione lo richiede, completi.

3.4. L'accesso e l'utilizzazione, da parte del datore di lavoro, di dati personali contenuti in un telefono cellulare, che siano registrati nella forma

di messaggi SMS o in altro formato, devono quindi rispettare queste massime del diritto generale (della LPD o della LPDP a dipendenza del rispettivo campo di applicazione), oltre a quelle eventualmente stabilite dal diritto speciale, settoriale (della protezione dei dati), che completa l'impianto giuridico applicabile in materia di tutela della personalità e della sfera privata.

Così, per quanto attiene all'ambito lavorativo privato, precise condizioni sono disciplinate in particolare agli art. 328 segg. del Codice delle obbligazioni (CO<sup>3</sup>, mentre per il personale dell'Amministrazione federale sono in particolare applicabili gli art. 27 segg. della legge sul personale federale (LPers<sup>4</sup>) e la relativa ordinanza sulla protezione dei dati del personale federale (OPDPers<sup>5</sup>), come pure, per quanto riguarda l'uso dell'infrastruttura elettronica del datore di lavoro, gli art. 57h segg. della legge federale sull'organizzazione del Governo e dell'Amministrazione (LOGA<sup>6</sup>), oltre alle disposizioni che tutelano la salute sul posto di lavoro, come specialmente l'art. 6 della legge federale sul lavoro (LL<sup>7</sup>) e l'art. 26 dell'ordinanza 3 concernente la LL (OLL 3<sup>8</sup>), disposto, quest'ultimo, incentrato peculiarmente sulla sorveglianza dei lavoratori. Per quanto attiene all'impiego pubblico cantonale, la legge sull'ordinamento degli impiegati dello Stato e dei docenti (LORD<sup>9</sup>) è molto generica in punto alla protezione della personalità, limitandosi infatti – ma comunque all'art. 1c cpv. 2 lett. g – a stabilire che lo Stato deve garantire la protezione della personalità e della salute nonché la sicurezza del personale sul posto di lavoro (secondo le disposizioni della LL e dell'OLL 3 appena citate). Per quanto desumibile, non vi sono però (ancora) norme specifiche di protezione della personalità in ambito di telefonia cellulare o fis-

---

<sup>3</sup> Legge di complemento del Codice civile svizzero (Libro quinto: Diritto delle obbligazioni) del 30 marzo 1911 (RS 220).

<sup>4</sup> Legge del 24 marzo 2000 (RS 172.220.1).

<sup>5</sup> Ordinanza del 26 ottobre 2011 (RS 172.220.111.4).

<sup>6</sup> Legge del 21 marzo 1997 (RS 172.10).

<sup>7</sup> Legge sul lavoro nell'industria, nell'artigianato e nel commercio del 13 marzo 1964 (RS 822.11).

<sup>8</sup> Ordinanza 3 del 18 agosto 1993 (Igiene, RS 822.113).

<sup>9</sup> Legge del 15 marzo 1995 (RL 2.5.4.1).

sa, anche se sono state emesse, per restare nell'ambito cantonale ticinese, delle direttive per la sicurezza e l'uso di risorse informatiche nell'Amministrazione cantonale<sup>10</sup>, che contemplano regole per l'uso autorizzato, senza però fornire indicazioni particolari sull'uso di SMS. Per quel che concerne i comuni, e le misure di loro competenza, il quadro normativo (anche di rango formale) può essere molto variegato. Esistono comunque, a diversi livelli, come a livello cantonale, direttive (di servizio) o atti analoghi, più o meno specifici, sull'uso dell'infrastruttura elettronica e quindi anche della telefonia fissa e mobile di servizio. Per quanto riguarda l'uso di SMS, esse sono anch'esse pressoché silenti.

3.5. Che siano di natura federale, cantonale o comunale, le disposizioni sulla protezione della personalità in ambito lavorativo valgono di principio per ogni rapporto di impiego, indipendentemente dallo statuto o anche dal ruolo particolare che il singolo dipendente può assumere in determinate circostanze: in questo senso, queste disposizioni tutelano di principio il collaboratore anche quando fa capo a strumenti di lavoro, e quindi anche a dispositivi elettronici, come quelli che presiedono alla comunicazione aziendale (interna ed esterna), anche in qualità di mittente o destinatario di messaggi SMS. La sfera personale o privata dell'impiegato è protetta indipendentemente dal diritto di proprietà sul cellulare di servizio.

#### **4. Condizioni per l'accesso e l'analisi di messaggi di telefonia cellulare**

4.1. Per quanto desumibile, le condizioni per l'accesso e l'analisi lecita di messaggi di telefonia cellulare dell'impiegato da parte del datore di lavoro non sono finora state oggetto di analisi giuridica puntuale, né nella dottrina né nella giurisprudenza svizzera e dei Paesi vicini, come neppure di approfondimenti di autorità in materia di protezione dei dati. Si può comunque sottolineare un punto fermo, ossia che il tema non è affatto sottratto al campo di applicazione della normativa generale sulla protezione dei dati, essendo quest'ultima tecnologicamente neutrale (art. 2

---

<sup>10</sup> Ris. gov. del Consiglio di Stato del Cantone Ticino n. 5133 del 24 ottobre 2006.

cpv. 2 LPD; art. 2 cpv. 1 LPDP). I principi generali della protezione dei dati possono essere applicati tracciando, dove possibile e indicato, dei paralleli con le norme applicabili ad elaborazioni di dati assimilabili a quella in discussione.

4.2. In questo senso è utile rilevare che, sebbene non siano completamente comparabili dal profilo tecnico, i messaggi SMS presentano molte analogie con i messaggi di posta elettronica (email), per cui, dove queste analogie esistono (ed entro inevitabili limiti), le regole della protezione dei dati possono essere applicate in misura corrispondente. Ora, in ambedue i casi, benché sulla base di tecnologie differenti, vengono trasmessi messaggi di testo, che possono essere oggetto di un salvataggio intermedio presso il provider, almeno fintanto che il messaggio non è stato consegnato al destinatario (sistema «*store & forward*»). L'analogia tra la posta elettronica e gli SMS appare qui evidente, in particolare in virtù del fatto che, in entrambi i casi, la comunicazione non presuppone la partecipazione simultanea di entrambi gli interlocutori (a differenza della telefonia o delle chat online). In effetti, tra l'invio, la ricezione e la lettura di un messaggio di posta elettronica o di un SMS può intercorrere un determinato lasso di tempo.

4.3. Le direttive dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) relative all'uso e alla sorveglianza della posta elettronica, contenute nella «*Guida alla sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro (per l'economia privata)*»<sup>11</sup>, possono dunque rappresentare uno spunto, o una fonte, da cui trarre delle regole per la messaggeria cellulare. Le direttive recenti dell'IFPDT – integrate dalle corrispondenti «*Informazioni sulla sorveglianza telefonica sul posto di lavoro*»<sup>12</sup> – non costituiscono però, come ovvio, un testo normativo, ma rappresentano comunque un ausilio interpretativo del diritto positivo inteso alla protezione della personalità<sup>13</sup>.

---

<sup>11</sup> Versione settembre 2013; pubblicata nel sito [www.lincaricato.ch](http://www.lincaricato.ch).

<sup>12</sup> Versione marzo 2004; pubblicata nel sito [www.lincaricato.ch](http://www.lincaricato.ch).

<sup>13</sup> DTF 139 II 7 consid. 5.5.1, GIORDANO COSTA, Internet und E-Mail-Überwachung am Arbeitsplatz, Entwicklungen in der Lehre, Rechtsprechung und Gesetzgebung, in Jusletter del 9 gennaio 2012, pag. 2 seg.

4.4. Queste direttive – che, finora almeno, non sono state contraddette o relativizzate nei punti principali dalla giurisprudenza e dalla dottrina, che anzi le hanno fatte proprie – stabiliscono innanzitutto che il datore di lavoro deve permettere all’impiegato che si appresta a concludere il rapporto di lavoro di cancellare dalla sua casella postale elettronica tutti i messaggi privati o personali prima di lasciare il posto di lavoro. Per motivi di sicurezza, il datore di lavoro conserva comunque il diritto di allestire una copia di sicurezza (backup) di tutta la posta elettronica (compresa dunque quella di carattere personale o privato, se gestita assieme a quella professionale), nonché la facoltà di assistere alla sua cancellazione, se sussiste il pericolo concreto che il dipendente possa ledere in qualche modo l’integrità e la confidenzialità della documentazione professionale. Se l’impiegato omette di cancellare i suoi documenti privati dai supporti di lavoro entro il giorno della sua partenza, gli va data la possibilità di farlo anche successivamente, dopo aver lasciato il posto di lavoro.

Per quanto riguarda invece l’accesso, da parte del datore di lavoro, alla posta elettronica dell’impiegato assente, le direttive raccomandano al datore di lavoro di regolamentarlo, unitamente al controllo<sup>14</sup>. A questo scopo, le direttive prevedono la presunzione della natura professionale dei messaggi di posta elettronica privi di elementi che li contraddistinguono chiaramente come privati. A dipendenza del regime previsto per l’uso privato dell’infrastruttura elettronica professionale – che può essere autorizzato, vietato (parzialmente o totalmente) o condizionato – la presunzione sulla natura, privata o professionale, del tipo di messaggi di posta elettronica può variare. In altre parole, nel caso in cui l’uso di dispositivi di servizio a scopo privato sia escluso esplicitamente e l’impiegato sia stato adeguatamente informato della facoltà di controllo del datore di lavoro e delle rispettive condizioni, quest’ultimo può presumere che ogni

---

<sup>14</sup> Sulla necessità di disciplinare a livello regolamentare l’elaborazione di dati personali da parte del datore di lavoro, vedi in particolare DAVID ROSENTHAL, *Datenschutz-Compliance im Unternehmen: Umsetzung in der Praxis und Handlungsbedarf des Gesetzgebers*, in Rolf H. Weber/Florent Thouvenin (ed.), *Neuer Regulierungsschub im Datenschutzrecht?*, Zurigo/Basilea/Ginevra 2012, pag. 157 segg., 164, 168; GIORDANO COSTA, *La sorveglianza sul posto di lavoro: occorrono nuove basi legali*, in RtiD I-2013, pag. 417 segg.

email in entrata o in uscita dalla casella di posta elettronica del collaboratore sia di natura professionale. Vi può quindi accedere in caso di necessità e urgenza (e queste condizioni sono spesso riunite in caso di assenza dell'impiegato), nella misura in cui le email private e/o personali non presentino un elemento distintivo (ad esempio una specifica menzione) che permette di qualificarle chiaramente come tali. Di conseguenza, in tali condizioni, il rinvenimento – anche fortuito – di dati personali di carattere privato da parte del datore di lavoro nell'ambito di un accesso alla mailbox professionale di un impiegato assente è considerato lecito e i dati possono, se del caso, essere utilizzati nell'ambito di ulteriori procedure<sup>15</sup>.

Nel caso in cui, invece, l'uso di dispositivi di servizio a scopo privato sia consentito, le direttive dell'IFPDT consigliano al datore di lavoro di dare prova di prudenza qualora intendesse accedere incondizionatamente al contenuto, in virtù dei dubbi oggettivi che possono evidenziarsi sulla natura di un messaggio, non potendone essere infatti essere esclusa a priori la natura privata. In particolare, le direttive suggeriscono di interpellare la persona interessata e ottenerne il consenso prima di accedere alla sua posta elettronica, sempre che, come già rilevato, non vi sia urgenza da parte del datore di lavoro. In altre parole, nel caso in cui l'uso di dispositivi di servizio a scopo privato sia consentito dal datore di lavoro, non è più data la presunzione della natura professionale del messaggio, e la sua ulteriore elaborazione non è più giustificata<sup>16</sup>. Se il datore di lavoro vi accede senza giustificazione (necessità e urgenza o consenso dell'interessato), può configurarsi una violazione illecita della sfera personale o privata dell'interessato. Tuttavia, anche in simili casi, in virtù di una ponderazione degli interessi, l'acquisizione di dati personali da parte del datore di lavoro può eccezionalmente essere considerata lecita se sono in gioco interessi preponderanti privati di terzi o pubblici quali, ad esempio, la necessità di chiarire una fattispecie per appurare se siano date le condizioni per dare avvio a una procedura disciplinare o per determinare la qualifica di atti illeciti (gravi).

---

<sup>15</sup> Vedi anche DAVID ROSENTHAL, in Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, Zurigo 2008, art. 328b OR, pag. 753 n. 77.

<sup>16</sup> Cfr. ROSENTHAL, op. cit., art. 328b OR, pag. 754 n. 78.

Se l'accesso da parte del datore di lavoro al contenuto del materiale di servizio restituito alla fine del rapporto di lavoro dipende dal consenso del collaboratore, occorre che quest'ultimo sia a conoscenza dell'esistenza di suoi documenti o di dati privati, o le circostanze obiettive permettano di presumerla.

4.5. In sé, non si intravedono ragioni oggettive per non applicare questi principi generali anche ai messaggi SMS. Se l'impiegato ignora che essi sono (ancora) memorizzati, il suo consenso all'accesso potrebbe essere considerato come non valido, poiché tale espressione di volontà, per essere giuridicamente vincolante, deve tra l'altro fondarsi su un'informazione sufficiente. Se invece l'impiegato è a conoscenza (o avrebbe dovuto esserlo con la dovuta diligenza) dell'esistenza degli SMS nella memoria del cellulare e può oggettivamente ritenere che essi potrebbero essere letti, il suo consenso (esplicito o per atti concludenti, come un suo disinteresse chiaramente manifestato) è da considerarsi di principio valido. Va comunque rilevato che nel settore lavorativo il consenso dell'impiegato ha una valenza più restrittiva rispetto ad altri ambiti, nel senso che vale unicamente nella misura in cui il diretto interessato non lo abbia dato a suo sfavore, cioè contro i suoi interessi (vedi art. 328 segg. e 362 CO combinati, per analogia).

4.6. Infine, sempre secondo le direttive dell'IFPDT, se l'uso privato degli strumenti di lavoro non è stato disciplinato, si può presumere – in virtù degli obblighi di diligenza e fedeltà dell'impiegato, rispettivamente di tutela degli interessi del datore di lavoro – che sussista un divieto dell'uso privato degli strumenti professionali, anche se, nella prassi, un uso razionale, proporzionato e comunque limitato è solitamente tollerato. Anche in questo caso il datore di lavoro non può accedere incondizionatamente ai messaggi del collaboratore, che siano email o messaggi SMS, ma unicamente in caso di urgenza e necessità per l'esecuzione del contratto di lavoro e in assenza di elementi che caratterizzano i messaggi chiaramente come privati o personali.

4.7. Oltre alla posizione dell'IFPDT, che finora almeno, è stata considerata determinante dalla giurisprudenza e dalla dottrina generale e speciale, esplicitata nelle direttive esposte sopra, è immaginabile anche una

concezione più severa, e intesa al divieto di partenza d'uso privato dell'infrastruttura professionale, come è il caso della Germania. Ma viste le numerose eccezioni poste dalla giurisprudenza a tutela della sfera privata dei collaboratori, il confronto tra le due visioni si riduce assai. Occorrerà quindi a questo punto osservare l'evoluzione in materia.

## **5. Valore probatorio di messaggi di telefonia cellulare**

5.1. L'integrità e l'autenticità di messaggi SMS, come pure di messaggi di posta elettronica, di fotografie digitali o altro, non sono di regola tecnicamente garantite, a meno che siano prese particolari misure per assicurarle (come, in particolare, la firma elettronica), adeguate a dipendenza del tipo di dispositivo. Se questi provvedimenti non sono adottati o se per motivi anche tecnici non possono essere attuati, il rischio di potenziali manipolazioni può oggettivamente esistere, soprattutto se terzi hanno potuto o possono accedere al supporto di dati. Nell'ambito di una procedura formale spetterà quindi all'autorità competente appurare, sulla base di propri accertamenti, l'integrità e l'autenticità di messaggi postati in formato elettronico, privi di certificati di sicurezza, qualora intendesse ammetterli come mezzi di prova ai fini della propria decisione.

5.2. Nel contesto si pone anche la questione di sapere se messaggi SMS acquisiti in violazione delle norme e delle disposizioni esposte in precedenza, riferite in modo particolare alla tutela della personalità e della sfera privata nell'ambito lavorativo, siano utilizzabili come mezzi di prova ai fini processuali. Sul piano normativo federale e cantonale, il tema dell'ammissibilità di prove ottenute illecitamente è stato viepiù codificato, seppur in maniera differenziata, nelle diverse procedure.

Nella procedura penale – fatti salvi i metodi probatori vietati enumerati all'art. 140 del codice di procedura penale (CPP<sup>17</sup>) che non possono essere usati in nessun caso (art. 141 cpv. 1 CPP) – l'art. 141 cpv. 2 della normativa stabilisce che le prove raccolte dalle autorità penali in modo penalmente illecito o in violazione di norme che ne condizionano la validità non possono essere utilizzate, eccetto che la loro utilizzazione sia

---

<sup>17</sup> Codice di diritto processuale penale svizzero del 5 ottobre 2007 (RS 312.0).

indispensabile per far luce su gravi reati. Per i procedimenti civili, l'art. 152 cpv. 2 del codice di procedura civile (CPC<sup>18</sup>) sancisce che il giudice prende in considerazione mezzi di prova ottenuti illecitamente soltanto se l'interesse all'accertamento della verità prevale. Queste disposizioni non contemplano peraltro nulla che non sia già riconosciuto dalla costante giurisprudenza del Tribunale federale, fondata sul diritto a un processo equo ai sensi degli art. 29 cpv. 1 della Costituzione federale (Cost.<sup>19</sup>) e 6 n. 1 CEDU<sup>20</sup>, che di principio – ma non in modo assoluto – vietano l'utilizzo di mezzi di prova acquisiti illecitamente<sup>21</sup>. L'eccezione – prefiguratasi recentemente soprattutto (ma non solo) in materia di utilizzo di registrazioni audio e video quale unico mezzo per accertare fatti talvolta gravi – riconosce l'ammissibilità di simili mezzi di prova soltanto a condizioni assai restrittive e con grande riserbo. L'autorità competente deve poi operare una ponderazione tra gli opposti interessi, che sono essenzialmente, da un lato, l'interesse all'accertamento della verità materiale e, dall'altro, l'interesse alla tutela della personalità, quale bene giuridico leso raccogliendo le prove in modo illecito<sup>22</sup>. Nell'ambito procedurale penale, come si è visto, il Tribunale federale ha invece riconosciuto il carattere preponderante dell'interesse pubblico all'accertamento e al perseguimento di un reato unicamente in merito a reati di particolare gravità.

Per quanto attiene, infine, alla procedura amministrativa – che non è unificata a livello svizzero come quella penale e civile – si applicano di principio le massime sviluppate dal Tribunale federale in materia di diritto civile, ritenuti appunto espressione del diritto a un processo equo

---

<sup>18</sup> Codice di diritto processuale civile svizzero del 19 dicembre 2008 (RS 272).

<sup>19</sup> Costituzione federale del 18 aprile 1999 (RS 101).

<sup>20</sup> Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950 (RS 0.101).

<sup>21</sup> DTF 139 II 7 consid. 6.4.1, 131 I 272 consid. 4 e relativi richiami; sul tema in generale: JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, 4<sup>th</sup> ed., Berna 2008, pag. 1003 segg., ALFRED KÖLZ/ISABELLE HÄNER/MARTIN BERTSCHI, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 3<sup>rd</sup> ed., Zurigo 2013, n. 480 seg., con rinvii a ulteriore giurisprudenza; LUCIE OTTINGER, L'exploitation des moyens de preuve obtenus illégalement: de la situation actuelle à celle du CPP unifié, in: Jusletter, 24 agosto 2009.

<sup>22</sup> DTF 139 II 7 consid. 6.4.1, 137 I 218 consid. 2.3, 131 I 272 consid. 4 e relativi rinvii.

garantito dall'art. 29 cpv. 1 Cost. e dall'art. 6 CEDU<sup>23</sup>. Vi sono comunque cantoni che si sono dotati di disposizioni più o meno precise in questo ambito. Tra questi anche il Cantone Ticino, che nella nuova legge di procedura amministrativa (LPAm<sup>24</sup>) ha inserito un articolo (il 29) che disciplina l'assunzione di prove ottenute illecitamente. Secondo questo disposto, l'autorità prende in considerazione mezzi di prova ottenuti illecitamente soltanto se l'interesse all'accertamento della verità prevale. Con l'art. 29 LPAm, che non era previsto nel messaggio governativo e che è stato accolto dopo un ampio dibattito in sede parlamentare, il legislatore ha fatto propria una considerazione del Tribunale federale – contenuta nella sentenza di principio DTF 139 II 7 – che evidenziava l'assenza nella previgente LPAm di una norma che disciplinasse l'uso di mezzi di prova acquisiti illecitamente, rinviando in modo generale alle norme della procedura civile. Il nuovo disposto colma quindi questa lacuna, recependo la corrispondente disposizione del CPC (art. 152 cpv. 2) e la relativa giurisprudenza del Tribunale federale, riconoscendo così la valenza pratica sempre più importante e crescente del tema anche in campo amministrativo (soprattutto quando un determinato riscontro è l'unico mezzo che permette di accertare fatti talvolta gravi). La disposizione parte dal principio assodato secondo cui il diritto alla prova non può di principio essere esercitato in modo illecito: così, mezzi di prova acquisiti illecitamente possono essere presi in considerazione soltanto a condizioni assai restrittive. Il mezzo di prova deve anzitutto essere ammissibile in quanto tale, ossia rientrare tra quelli inclusi nell'elenco esaustivo dell'art. 28 LPAm. L'autorità competente deve poi procedere a una ponderazione tra, da un lato, l'interesse alla tutela del bene giuridico leso raccogliendo le prove in modo illecito e, dall'altro, l'interesse all'accertamento della verità. In conformità alla giurisprudenza recente del

---

<sup>23</sup> DTF 139 II 7 consid. 6.2.

<sup>24</sup> Legge del 24 settembre 2013, in vigore dal 1° marzo 2014 (RL 3.3.1.1), che ha sostituito previgente legge del 1966 (vedi messaggio n. 6645 del 23 maggio 2012 concernente la revisione totale della legge di procedura per le cause amministrative del 19 aprile 1966 e rapporto n. 6645R del 4 settembre 2013 della Commissione della legislazione sul messaggio citato).

Tribunale federale<sup>25</sup> un documento estorto con minacce o con la violenza non è utilizzabile, giacché in linea di principio l'integrità personale prevale sull'interesse all'accertamento della verità. All'opposto un documento sottratto può essere preso in considerazione se l'interesse alla verità prevale<sup>26</sup>. Un mezzo di prova non può invece essere preso in considerazione se il fatto può essere provato in modo lecito oppure lo può con una misura meno invasiva, più rispettosa della sfera privata e della personalità della persona interessata, come già esige del resto il principio di proporzionalità. L'utilizzo di mezzi di prova acquisiti in seguito a un'ingerenza illecita (soprattutto nella sfera privata) dev'essere in ogni caso ammesso solo con grande riserbo<sup>27</sup>.

5.3. Anche l'ammissibilità di messaggi SMS (raccolti illecitamente) quali prove ai fini processuali va vagliata alla luce delle descritte condizioni. La loro ammissibilità dipende anche dal tipo di procedura avviata: come detto, nella procedura penale – rispetto a quella civile e a quella amministrativa – le condizioni sono più severe, costituendo il requisito della gravità del reato un elemento centrale (e quest'ultimo, nel caso di invio/ricezione di SMS, potrebbe molto spesso anche non essere adempiuto). A ciò aggiungansi le riserve esposte in ordine all'integrità e autenticità, e quindi all'affidabilità dei messaggi, che dipende dall'esame di diverse variabili in ogni singolo caso. In definitiva, ben può dirsi che il valore probatorio dei messaggi dipende essenzialmente dal grado di convincimento dell'autorità competente, ritenuto in ogni caso che un'eventuale ammissibilità deve essere ammessa, e va ribadito, solo a titolo eccezionale.

## 6. Conclusioni

Malgrado il mercato proponga a getto continuo nuovi dispositivi per la telefonia mobile con funzionalità sempre più ampie e performanti, la messaggia SMS continua a essere, per la sua facilità d'uso, uno stru-

---

<sup>25</sup> Cfr. DTF 136 V 117 consid. 4.2.2, 131 I 272 consid. 4.

<sup>26</sup> Vedi anche messaggio del 28 giugno 2006 del Consiglio federale relativo al nuovo CPC; (FF 2006 6593, 6685).

<sup>27</sup> Rapporto n. 6645R cit., commento all'art. 29.

mento comunicativo ampiamente utilizzato. Nell'ambito professionale non si può escludere che messaggi di questa natura possano rivestire un certo interesse per il datore di lavoro, soprattutto ove si tratti di appurare dei fatti attinenti la sfera lavorativa. Egli può tuttavia acquisire e utilizzare i messaggi dei propri collaboratori solo rispettando il quadro legale e i principi generali statuiti dalle normative sulla protezione dei dati e da quelle intese a regolamentare il rapporto d'impiego. Il *Short Message System* può presentare analogie con la posta elettronica (Email). Laddove queste analogie esistono, le regole della protezione dei dati riferite alla posta elettronica possono essere applicate in misura corrispondente. Ciò significa che anche il sistema di presunzioni riguardanti la natura privata o professionale dei messaggi, predisposto per la posta elettronica, può essere applicato alla messaggeria SMS. Un eventuale consenso dell'impiegato all'accesso deve essere libero e informato. L'accessibilità dipende, tecnicamente, anche dalla tipologia di informazioni e dal tipo di dispositivo che le contiene (con le funzionalità che gli sono proprie). Il potenziale valore probatorio di SMS dipende essenzialmente dal grado di autenticità e di integrità dei messaggi, che va appurata alla luce delle circostanze del caso specifico. Qualora i dati siano raccolti in modo illecito dal datore di lavoro, la loro ammissibilità in sede penale, amministrativa o civile va ammessa – secondo il diritto processuale applicabile, conformemente alla prassi del Tribunale federale – solo restrittivamente e solo nel caso in cui siano adempiute precise condizioni, che presiedono anche a una ponderazione di interessi contrapposti.

In definitiva, gli elementi da appurare sono molteplici e d'esito incerto quanto alla loro pertinenza. Una facilitazione per il datore di lavoro confrontato con situazioni di questo tipo è certamente quella di disporre di un quadro normativo almeno interno, adeguato alla realtà aziendale o amministrativa che, da un lato, regolamenti in modo puntuale l'uso di tutti i dispositivi di servizio in dotazione degli impiegati, che definisca in particolare le autorizzazioni rilasciate ai collaboratori e dia indicazioni precise sul controllo dell'uso e le relative modalità e, dall'altro, preveda anche disposizioni a tutela della personalità e della salute del personale sul posto di lavoro.