LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 4 /
2021

Paola
Borghi

Protocollo nazionale sul lavoro in modalità agile e tutela della riservatezza: prime riflessioni e spunti operativi

Protocollo nazionale sul lavoro in modalità agile e tutela della riservatezza: prime riflessioni e spunti operativi

Paola Borghi

Sommario: 1. Premessa: lavoro in modalità agile e privacy. – 2. Profili generali. – 3. Prescrizioni specifiche. – 3.1. Il luogo di lavoro. – 3.2. Gli strumenti di lavoro. – 3.3. Gli obblighi del datore di lavoro. – 3.4. Gli obblighi del lavoratore.

1. Premessa: lavoro in modalità agile e privacy

Il Protocollo dedica un'ampia e specifica attenzione alla tematica della riservatezza e della protezione dei dati personali, disegnando un quadro di riferimento in cui trovano piena cittadinanza i principi rivenienti dal Regolamento europeo 2016/679 (GDPR), dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, come modificato ed integrato dal d.lgs. 10 agosto 2018, n. 101), nonché dalle Linee guida dei Garanti europei e del Garante nazionale.

Ne deriva la previsione di un'insieme di disposizioni che, in ragione della loro portata e delle connesse implicazioni, vedono coinvolti tanto i datori di lavoro, quanto i lavoratori, entrambi chiamati ad operare attivamente per realizzare il contemperamento e/o bilanciamento tra l'interesse legittimo dell'uno, a proteggere la propria attività e quello, dell'altro, alla ragionevole aspettativa di protezione della propria vita privata.

Contemperamento che, a ben vedere, rappresenta, nell'attuale contesto storico, una vera sfida, posto che l'adozione di tecnologie sempre più sofisticate, che consentono nuovi tipi di trattamento sistematico di dati potenzialmente invasivi, hanno, tra l'altro, reso più labili i confini tra

l'ambito domestico e quello lavorativo. E ciò, come rilevato dai Garanti europei nel Parere 2/2017 sul trattamento dei dati sul posto di lavoro[1] , è tanto più vero con riferimento ai dipendenti che lavorano da remoto, potendo configurarsi in questo caso «un monitoraggio delle attività al di fuori dell'ambiente fisico di lavoro che può includere potenzialmente il monitoraggio di una persona in un contesto privato».

Del resto, si evidenzia nel medesimo documento, il lavoro a distanza «presenta un rischio aggiuntivo per il datore di lavoro», dal momento che i dipendenti che hanno accesso remoto all'infrastruttura del datore di lavoro, non sono vincolati alle misure fisiche di sicurezza che possono essere messe in atto presso i locali del datore di lavoro. Da ciò la necessità dell'adozione di specifiche e puntuali misure tecniche ed organizzative adeguate ai rischi connessi con lo svolgimento del lavoro in tale modalità.

La predisposizione di tali misure tecniche ed organizzative – che rappresenta invero la chiave di volta del sistema in esame, come meglio si vedrà nell'analisi del Protocollo – presuppone naturalmente il rispetto dei principi fondamentali posti dal Regolamento europeo: conseguentemente i datori di lavoro dovranno garantire che i dati siano trattati per finalità specifiche e legittime, proporzionate e necessarie, che siano adeguati, pertinenti e non eccessivi rispetto alle finalità previste e che siano rispettati nel trattamento i principi di proporzionalità e trasparenza.

In proposito, è opportuno ricordare che tali principi, come noto, sono richiamati anche dall'art. 4, comma 3, l. n. 300 del 1970 che, nel testo introdotto dal Jobs Act, subordina, l'utilizzo a tutti i fini delle informazioni raccolte tramite i sistemi tecnologici, al rispetto, oltre che dell'informazione adeguata, dei predetti principi rivenienti dal Regolamento europeo e dalla normativa nazionale.

[1] Gruppo di lavoro Articolo 29 per la protezione dei dati, Parere n. 2/2017 sul trattamento dei dati sul posto di lavoro, adottato l'8 giugno 2017, WP 249.

Da quanto molto sommariamente esposto, risulta evidente un mosaico in cui i vari tasselli rappresentati da utilizzo di strumenti elettronici, controlli, monitoraggi, devono comporsi in modo da garantire il necessario equilibrio tra esigenze produttive e tutela della vita privata del lavoratore; vita privata che, come insegna la Corte EDU, deve essere intesa in senso ampio, ricomprendendo l'art. 8 della CEDU tutte le attività che consentono lo sviluppo della personalità e la vita di relazione, «il cui esercizio sul luogo di lavoro non potrebbe in ogni caso essere ridotto a zero»[2].

2. Profili generali

La tematica della riservatezza e della protezione dei dati personali permea l'intero articolato del Protocollo: sebbene, infatti, sia dedicato un articolo specifico a tali profili (art. 12), indicazioni e principi in materia si rinvengono anche in altre disposizioni che disciplinano lo svolgimento del lavoro in modalità agile.

Il che evidenzia immediatamente la sensibilità delle Parti sociali sull'argomento che hanno, del resto, stabilito di ritenere «necessario gestire lo sviluppo digitale attraverso un utilizzo appropriato della tecnologia, evitando qualsiasi forma di invasione della vita privata, nel pieno rispetto della persona» (art. 13, comma 4).

Va altresì osservato, sempre a livello generale, che viene stabilito che «resta ferma la normativa vigente sul trattamento dei dati personali e, in particolare, il Regolamento UE 679/2016 (GDPR)» (art. 12, comma 3): ne consegue che sembra ragionevole qualificare le previsioni rivenienti dal Protocollo alla stregua di norme speciali rispetto alla disciplina generale. Esse pertanto, si aggiungono, e non si sostituiscono agli altri principi e alle altre norme in materia.

[2] Grande Camera della Corte europea dei Diritti dell'Uomo, 5 settembre 2017, in causa Barbulescu c. Romania, n. 61496/08

Sempre a livello di inquadramento generale, merita segnalazione un ulteriore profilo di particolare rilevanza, connesso alla necessità, evidenziata dalle Parti sociali, di adottare un codice deontologico e di buona condotta per il trattamento dei dati personali dei lavoratori in modalità agile, da sottoporre al giudizio di conformità da parte dell'Autorità garante (art. 12, comma 6).

La previsione, di particolare rilievo in una prospettiva *de iure condendo,* deve essere letta in combinato disposto con quanto previsto dall'art. 111 del d.lgs. 196 del 2003, come modificato dal d.lgs. 101 del 2018, in base al quale il Garante promuove l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'art. 88 del Regolamento[3].

In proposito, va comunque ricordato che, sebbene già nella vigenza del precedente Codice privacy (antecedente all'entrata in vigore del Regolamento europeo) fosse prevista l'adozione di codici di deontologia nella materia del lavoro, non risulta che siano state attivate iniziative in tal senso. La necessità sottolineata ora dalle Parti sociali potrebbe, dunque rappresentare un *input* significativo per l'avvio dell'adozione di misure di tal tipo che indubbiamente, stante la loro specificità, potrebbero essere di ausilio nella gestione delle questioni connesse allo svolgimento del rapporto di lavoro, in generale, e di quello in modalità agile, in particolare.

3. Prescrizioni specifiche

Venendo all'esame specifico delle varie previsioni, si ritiene opportuno, per comodità di analisi, accorpare le prescrizioni dettate in materia di tutela

[3] La legislazione italiana, con la previsione di cui all'art. 111 conferisce al Garante la legittimazione a promuovere le «regole deontologiche per i trattamenti nell'ambito del rapporto di lavoro» nell'ambito delle finalità indicate dall'art. 88 del Regolamento. In proposito, occorre tuttavia sottolineare che l'art. 88 richiamato, attribuisce agli Stati membri il compito di prevedere, tramite leggi o contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro.

della riservatezza, secondo quattro aree tematiche: luogo di lavoro, strumenti di lavoro, obblighi del datore di lavoro, obblighi del lavoratore.

3.1. Il luogo di lavoro

La questione dell'individuazione del luogo di lavoro viene affrontata in più disposizioni: art. 2, comma 2, lett. C), relativo al contenuto dell'accordo individuale, dove è previsto che devono essere indicati «i luoghi eventualmente esclusi per lo svolgimento della prestazione lavorativa esterna ai locali aziendali»; art. 4, comma 1, secondo cui «il lavoratore è libero di individuare il luogo ove svolgere la prestazione in modalità agile purché lo stesso abbia caratteristiche tali da consentire la regolare esecuzione della prestazione, in condizioni di sicurezza e riservatezza, anche con specifico riferimento al trattamento dei dati e delle informazioni aziendali nonché alle esigenze di connessione con i sistemi aziendali»; art. 4, comma 2, secondo cui «la contrattazione collettiva può individuare i luoghi inidonei allo svolgimento del lavoro in modalità agile per motivi di sicurezza personale o protezione, segretezza e riservatezza dei dati»; art. 6, comma 3, a norma del quale «la prestazione effettuata in modalità di lavoro agile deve essere svolta esclusivamente in ambienti idonei, ai sensi della normativa vigente in tema di salute e sicurezza e per ragione dell'esigenza di riservatezza dei dati trattati».

Dall'analisi di tali disposizioni, fatte salve le questioni di salute e sicurezza, estranee al presente commento, risulta che il luogo in cui si svolge il lavoro in modalità agile è qualificabile come "idoneo" allorquando sussistano le condizioni che assicurino/garantiscano la riservatezza e la segretezza dei dati. Declinando questa previsione sul piano pratico, si potrebbe pertanto ipotizzare di ritenere inidoneo il luogo in cui i dati siano visibili e/o conoscibili e/o udibili e/o percepibili a terzi estranei; così come potrebbe ritenersi inidoneo, ad esempio, un luogo in cui ci si colleghi ad una rete di un locale pubblico o di un privato che non abbia sufficienti garanzie, anche

per quanto riguarda l'adozione di misure di sicurezza. In questi casi, il rischio di perdite o violazioni di dati personali (*data breach*) potrebbe essere elevato e probabile e potenzialmente foriero di responsabilità per il datore di lavoro e il lavoratore.

È pertanto necessario che il lavoratore venga informato e reso consapevole dei rischi derivanti dall'utilizzo improprio degli strumenti di lavoro e sulle conseguenze che ne possono derivare, anche rispetto ai profili appena delineati, attraverso iniziative di formazione e di sensibilizzazione esplicitamente previste dalle Parti sociali (v. *infra).*

3.2. Gli strumenti di lavoro

La strumentazione tecnologica e informatica necessaria allo svolgimento della prestazione lavorativa in modalità agile, viene definita, dallo stesso Protocollo, «strumenti di lavoro».

Tralasciando in questa sede la complessa questione relativa all'individuazione concreta degli strumenti tecnologici che possono qualificarsi come «strumenti di lavoro» – su cui, com'è noto, si rinvengono numerosi (e non sempre univoci) interventi da parte della dottrina, della giurisprudenza di legittimità e di merito, del garante per la protezione dei dati personali, dell'Ispettorato nazionale del lavoro – ritengo di soffermarmi su alcuni specifici aspetti direttamente connessi alla protezione dei dati personali.

Tra gli strumenti di lavoro rientrano certamente l'utilizzo di internet e della posta elettronica, nonché l'utilizzo dei pc/*device*/cellulari aziendali, dotati di applicazioni e programmi: sul punto, è opportuno sottolineare che i datori di lavoro, nel fornire indicazioni circa l'utilizzo di tali strumenti dovranno, anche con riferimento al lavoro in modalità agile, attenersi ai principi e alle prescrizioni rivenienti nelle Linee guida su internet e la posta elettronica emanate dal Garante nel marzo del 2007. Si ritiene, infatti, che anche successivamente all'entrata in vigore del Regolamento europeo, tali

Linee guida conservino la loro funzione di indirizzo e prescrittiva, risultando «perfettamente in linea con lo spirito di prevenzione del rischio che il Regolamento pone a base del nuovo sistema di regole tramite il principio di *accountability* e l'esigenza della realizzazione delle modalità di trattamento tramite i meccanismi della privacy *by design* e *by default*»[4].

Va altresì sottolineato che il richiamo ai principi del d.lgs. 196 del 2003 operato dal predetto terzo comma dell'art. 4, deve ritenersi comprensivo, come sopra accennato, anche della normativa di cui al Regolamento. Ne risulta, che l'utilizzo a tutti i fini connessi al rapporto di lavoro delle informazioni raccolte, presuppone sia il rispetto di tutte le garanzie e i limiti dettati in tema di protezione dei dati personali, sia l'adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli[5].

Informazione che viene considerata specificatamente dalle Parti sociali: è, infatti, previsto che il datore di lavoro «deve fornire, per iscritto, al lavoratore in modalità agile tutte le informazioni adeguate sui controlli che possono essere effettuate sul trattamento dei dati personali, come previsto dalla normativa vigente» (art. 13, comma 6).

3.3. Gli obblighi del datore di lavoro

Sul datore di lavoro incombono una serie di adempimenti che riguardano, da un lato, i dati trattati **dei** lavoratori in modalità agile, dall'altro i dati trattati **dai** lavoratori in modalità agile.

Con riferimento al primo aspetto, il datore di lavoro, oltre alle adeguate informazioni scritte sui controlli che possono essere effettuate sul trattamento dei dati personali dei lavoratori, già citate, è tenuto: a) ad adottare tutte le misure tecnico-organizzative adeguate per garantire la

[4] A. Maresca - S. Ciucciovino - I. Alvino, *Regolamento UE 2016/679 e rapporto di lavoro*, in L. Califano - C. Colapietro, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, p. 344.

[5] Occorre precisare che l'adeguata informazione di cui al terzo comma dell'art. 4 è un atto distinto e diverso dall'informazione fornita ai lavoratori ai sensi degli artt. 13 e 14 del Regolamento.

protezione dei dati dei lavoratori in modalità agile (art. 12, comma 2); b) ad informare i medesimi lavoratori in merito ai trattamenti di dati che li riguardano, anche nel rispetto delle previsioni dell'art. 4 l.n. 300 del 1970 (art. 12, comma 4, primo periodo).

Il datore di lavoro, quindi, è chiamato a predisporre un "pacchetto" specifico, una serie di misure dedicate in cui gli interessi delle parti dovranno ovviamente essere contemperati.

Passando alla protezione dei dati trattati **dai** lavoratori, il Protocollo innanzi stabilisce che il datore di lavoro deve adottare le misure tecniche ed organizzative adeguate per garantire la protezione dei dati trattati dai lavoratori agili (art. 12, comma 2) ed è tenuto a fornire ai medesimi lavoratori le istruzioni e le indicazioni delle misure di sicurezza che gli stessi dovranno osservare per garantire la protezione, la segretezza e la riservatezza delle informazioni che trattano per fini professionali (art. 12, comma 4, secondo periodo).

Il datore di lavoro dovrà, in sostanza, rivedere ed implementare gli atti interni/i regolamenti/le policy esistenti con previsioni specifiche giustificate dalla modalità di svolgimento del rapporto.

Ma quale dovrebbe essere il contenuto di tali previsioni? Quali sono, in concreto, le istruzioni, le indicazioni che devono essere fornite ai lavoratori?

Un supporto alla soluzione di questi interrogativi, sembrerebbe ragionevolmente rinvenirsi da quanto previsto nel comma 5 dell'art. 12, laddove è previsto che il datore di lavoro promuove l'adozione di *policy* aziendali basate sul concetto di *security by design* e favorisce iniziative di formazione e di sensibilizzazione dei lavoratori. In realtà, in questa previsione, è specificato che le *policy* prevedono la gestione dei *data breach* e l'implementazione di misure di sicurezza adeguate quali, ad esempio, la crittografia, sistemi di autenticazione e VPN, piani di *backup* e protezione *malware*. Allo stesso modo viene esplicitato che la formazione e la

sensibilizzazione dei lavoratori deve avere ad oggetto l'utilizzo, la custodia e la protezione degli strumenti utilizzati per rendere la prestazione, le cautele comportamentali, la gestione dei *data breach.*

In altre parole, il Protocollo fornisce già delle indicazioni concrete e operative su quelli che dovranno/potranno essere le previsioni aggiuntive da inserire nei regolamenti/atti interni/policy esistenti.

Occorre ricordare in proposito che questi regolamenti e/o policy aziendali si configurano quali atti unilaterali, con una valenza equiparata agli ordini di servizio: la loro inosservanza, pertanto, dà luogo all'applicazione di sanzioni disciplinari.

È conseguentemente necessario che le modifiche ed integrazioni apportate a tali regolamenti/atti interni in ragione dello svolgimento in modalità agile, siano portati a conoscenza di tutti i lavoratori con le modalità che si riterranno più opportune, ma comunque idonee a garantirne una conoscenza generalizzata. Per le medesime ragioni, si ritiene che gli stessi siano oggetto di illustrazione ed analisi nell'ambito della formazione.

Formazione che, nel Protocollo assume una particolare rilevanza: è infatti stabilito che «resta fermo ed impregiudicato **il diritto alla formazione c.d.obbligatoria** in materia di tutela della salute dei lavoratori e di protezione dei dati, da erogarsi nelle modalità più coerenti con lo svolgimento del lavoro agile» (art. 13, comma 5).

La previsione merita un *focus,* per la qualificazione della formazione in materia di protezione dei dati personali come obbligatoria. In realtà, tale obbligatorietà, a differenza di quanto previsto per la materia della salute e sicurezza di lavoratori, non si rinviene in alcun previsione normativa, anche se il Garante in più occasioni ha avuto modo di sottolineare la rilevanza e l'importanza della formazione in questa materia.

Si può dunque ritenere che tale formazione seppur non obbligatoria per legge, è fortemente incentivata e raccomandata dalle Parti sociali, valutati i vari aspetti in tema di riservatezza rilevanti in tale contesto.

Formazione che viene promossa innanzi tutto per una finalità di «uso responsabile delle apparecchiature tecnologiche» (art. 13, comma 4, secondo periodo), e che in ogni caso dovrà riguardare le istruzioni e le misure di sicurezza che il lavoratore dovrà adottare e dovrà sensibilizzare i lavoratori «sia sull'utilizzo, custodia e protezione dei strumenti impiegati per rendere la prestazione lavorativa in modalità agile» (art. 12, comma 5), sia, come sopra visto, «sulle cautele comportamentali da adottare».

Gli ulteriori obblighi posti a carico del datore di lavoro, sono connessi al suo ruolo di Titolare del trattamento.

Le Parti sociali, muovendo dal principio di *accountability* (responsabilizzazione) del titolare introdotto dal Regolamento europeo, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento europeo, pongono l'accento sulla necessità di verificare che gli strumenti utilizzati per il lavoro in modalità agile siano conformi al principio di *privacy by default and by design*. Ne consegue che il titolare/datore di lavoro sarà tenuto a verificare, fin dalla progettazione, le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

È previsto quindi, che prima di procedere al trattamento, il titolare/datore di lavoro effettui la valutazione di impatto sui trattamenti ai sensi dell'art. 35 del Regolamento. E ciò in coerenza con la disciplina generale, avendo il Garante, con Provvedimento n. 467 dell'11 ottobre 2018, relativo all'elenco delle tipologie dei trattamenti soggetti alla valutazione di impatto, indicato, tra gli altri, proprio i «trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai

sistemi di video sorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei lavoratori». Il titolare/datore di lavoro sarà inoltre tenuto all'aggiornamento del registro dei trattamenti dei dati connessi alle attività svolte anche in modalità di lavoro agile, così come all'implementazione delle misure di sicurezza adeguate al rischio. In proposito si ricorda che, a differenza dell'impianto normativo antecedente all'entrata in vigore del Regolamento, non è allo stato previsto un elenco delle misure di sicurezza da adottare, essendo rimessa la loro adozione, alla responsabilità del titolare del trattamento.

Sarà dunque obbligo del titolare individuare, così come previsto dall'art. 32 del Regolamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, dei rischi di probabilità e gravità per i diritti e le libertà delle persone fisiche, le misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio.

E in proposito il Protocollo, a titolo esemplificativo, come già evidenziato, richiama i sistemi di crittografia dei dati, l'utilizzo di specifici criteri di autenticazione, una rete dedicata, sistemi di backup e di protezione dai virus.

Un discorso a parte merita l'attenzione rivolta dalle Parti sociali al fenomeno del *data breach*, ovvero all'ipotesi di una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Considerato che una violazione siffatta può evidentemente compromettere la riservatezza, l'integrità o la disponibilità dei dati, è previsto, come anticipato, che il datore di lavoro deve adottare *policy* aziendali e favorire iniziative di formazione e sensibilizzazione relative alla gestione dei d*ata breach*. E in tale contesto, potrebbero, ad esempio, risultare utili e/o opportuni

specifiche attività formative in tema di *phishing* e *ransomware*, risultando, allo stato, le principali cause dei *data breach* denunciati e/o conosciuti.

3.4. Gli obblighi del lavoratore

L'attività di formazione e di sensibilizzazione relative alla gestione dei *data breach* acquista particolare rilevanza qualora si consideri che grava sui lavoratori l'obbligo di attivare la procedura aziendale per la gestione degli stessi «in caso di guasto, furto o smarrimento» degli strumenti di lavoro.
Sul lavoratore grava inoltre l'obbligo di trattare i dati cui accede per finalità connesse allo svolgimento della propria prestazione lavorativa secondo le istruzioni impartite dal datore di lavoro, assicurando la riservatezza sui dati e sulle informazioni aziendali in possesso o disponibili sul sistema informatico aziendale.
Il lavoratore dovrà quindi operare in adempimento di quanto previsto nel regolamento aziendale e/o policy aziendali, e pur sempre nel rispetto dei generali principi di correttezza e buona fede.