

*Verbale di Accordo sull'uso di sistemi informatici
ai sensi dell'art.4, comma 1 della Legge n.300/70*

Roma, 22 ottobre 2020

Tra TIM S.p.A.

e

*il Coordinamento Nazionale RSU TIM unitamente alle Segreterie Nazionali SLC-CGIL,
FISTel-CISL, UILCOM-UIL, UGL Telecomunicazioni*

Premesso che

- Il 26 marzo 2020 sono stati siglati due accordi sindacali per l'avvio di una sperimentazione, rispettivamente nelle regioni Calabria e Toscana, relativa alla realizzazione di un sistema elettronico per l'apertura controllata degli armadi ripartilinea stradali, rispondente ad esigenze organizzative e produttive, nonché di tutela del patrimonio aziendale (Sistema SmartLocker);
- nei territori sopra menzionati sono state completate circa 2.300 installazioni (di cui ca. 1.100 attive in Toscana e ca. 1.200 attive in Calabria);
- nei mesi di sperimentazione è stata rilevata una significativa riduzione dei fenomeni anomali/dolosi (da maggio sono state rilevate 5 forzature serratura, 2 in Calabria e 3 in Toscana);
- i dati relativi agli accessi alla infrastruttura di rete (centrali, locali permutatori, ecc.) provvista di controllo apertura porte tramite badge vengono raccolti sui data base della Control Room Security;
- il Sistema SmartLocker consentirà attraverso l'installazione di appositi sensori, di monitorare da remoto lo stato dell'armadio ripartilinea misurando diversi parametri (quali ad esempio: temperatura, umidità, presenza di energia elettrica) che consentiranno tempestivi interventi di manutenzione ancor prima che si verifichino dei guasti;
- la messa in sicurezza dell'infrastruttura di rete e in generale la difesa del patrimonio di TIM diventa un tema ancor più prioritario in considerazione della progressiva attuazione delibera AGCOM sulla disaggregazione delle attività wholesale che determinerà l'accesso agli elementi di rete ad un numero sempre maggiore di tecnici appartenenti alle aziende esterne;
- nell'ottica del futuro sviluppo della rete dove gli armadi ripartilinea rappresentano un punto nodale del suo funzionamento e consolidamento, l'Azienda si impegna ove necessario ad assicurare la manutenzione degli stessi. Con cadenza annuale TIM, sulla base di priorità di intervento, effettua tramite i propri tecnici (MOS) una verifica tecnica sui circa 150.000 armadi presenti sul territorio nazionale che si risolve, se

necessario, con interventi di bonifica (es. Cambio sportello, serratura, riordino permutate, pulizie testine etc.). I dati relativi agli armadi verificati vengono sistematicamente trasmessi ad AGCOM;

- ai sensi dell'art.4, legge n.300/1970, comma 1, gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, previo accordo sindacale.

Tutto ciò premesso si conviene quanto segue:

A seguito dell'esito positivo della sperimentazione effettuata nelle regioni Calabria e Toscana, l'installazione del Sistema SmartLocker sarà estesa sull'intero territorio nazionale secondo i criteri di seguito definiti.

1. Adozione ed implementazione del Sistema SmartLocker

- 1.1. L'apertura degli armadi ripartilinea stradali sarà consentita al solo personale tecnico abilitato (sia personale TIM che esterno) tramite una specifica procedura. La serratura dell'armadio sarà sbloccata dalla Olivetti "console SmartLocker", attraverso l'utilizzo dell'apposita APP, solo se il tecnico sarà riconosciuto tra quelli abilitati.
- 1.2. L'APP non funzionerà in background, pertanto per poter sbloccare la porta dell'armadio ripartilinea il lavoratore dovrà avviarla sul proprio cellulare. L'APP, a valle dell'autorizzazione ricevuta dalla console SmartLocker, permetterà al tecnico, tramite connessione Bluetooth, di identificare, l'armadio a cui accedere e del quale sbloccare la serratura, consentendo l'apertura dello sportello.
- 1.3. I dati personali (matricola del tecnico) relativi alle transazioni di accesso all'armadio, unitamente all'identificativo dell'armadio, confluiranno, per la tutela del patrimonio, sui data base in uso presso la Control Room Security (PHOTOBASE ed ERASWEB e relativi sviluppi), in analogia a quanto avviene per altri importanti elementi di rete (ad esempio, centrali, permutatori, ecc.).
- 1.4. Le informazioni relative agli eventi occorsi nei singoli armadi (ora, apertura/chiusura, identificativo univoco associato all'armadio) saranno archiviate sul datawarehouse di Chief Operations Office (Opera). Tali dati saranno utilizzati per elaborare report aggregati sulle attività di apertura/chiusura, anche al fine di consentire eventuali correlazioni tra gli eventi e l'insorgenza di guasti al ripartilinea.
- 1.5. Il sistema informatico centralizzato di Olivetti "console SmartLocker" memorizzerà i dati di accesso agli armadi ripartilinea per il solo tempo necessario all'invio ai database di TIM di cui ai precedenti punti 1.3 e 1.4, comunque secondo i tempi previsti dal successivo paragrafo 4.3.

2. **Soggetti legittimati all'accesso dei dati**

- 2.1. I dati di cui al punto 1.3 saranno accessibili solo dalla struttura nazionale Control Room Security in ambito Security e dalle strutture Physical Security territoriali (Nord, Centro e Sud). Su segnalazione dell'Autorità Giudiziaria o di Pubblica Sicurezza, ovvero nell'evidenza di incidenti di sicurezza o azioni compiute in frode alla legge o a danno del patrimonio aziendale, la Funzione HRO competente potrà richiedere alla funzione Security di fornire i dati in chiaro del personale che ha effettuato l'accesso all'armadio ripartilinea oggetto dell'evento.
- 2.2. I dati di cui al punto 1.4 saranno a disposizione delle strutture deputate alle attività di Maintenance e Technical Infrastructure, Technical Planning e Operational Planning di Chief Operations Office.
- 2.3. Gli Amministratori di Sistema (Olivetti), appositamente designati, ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 in materia di "Misure ed accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", sono identificati come unici soggetti autorizzati ad accedere ai dati in chiaro e al trattamento dei relativi dati trattati sulla piattaforma Olivetti "console SmartLocker". Gli amministratori di sistema sono tenuti al rispetto delle policy, delle procedure e delle disposizioni aziendali in materia di sicurezza e di gestione degli accessi ai sistemi informatici.

3. **Utilizzo dei dati**

- 3.1. I dati raccolti saranno trattati secondo la disciplina dettata dal D. Lgs 196/03 novellato dal D.Lgs 101/18 e Regolamento 2016/679/UE in materia di protezione dei dati personali, nonché secondo la disciplina lavoristica in materia di impiego di "strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori" ex art. 4, della Legge n. 300/1970 come modificato dall'art. 23 D.lgs n. 151/2015. I dati raccolti non potranno essere utilizzati al fine di verificare il corretto adempimento della prestazione lavorativa e pertanto non potranno essere diffusi in altri ambiti aziendali. Solo in caso di comprovata ricorrenza di fattispecie costituente possibile reato, denunciata all'autorità Giudiziaria o di Pubblica Sicurezza, i dati potranno essere usati ai fini disciplinari.

4. **Conservazione dei dati**

- 4.1. I dati di cui al punto 1.3, tenuto conto dei tempi relativi alle possibili contestazioni e alle conseguenti indagini da parte degli organi giudiziari, saranno conservati per massimo 6 mesi.
- 4.2. I dati di cui al punto 1.4 saranno conservati per 6 mesi.
- 4.3. I dati di cui al punto 1.5 saranno conservati per il tempo necessario al trasferimento ai database di cui al punto 1.3, di norma per massimo 24 ore.

5. Informativa

- 5.1. In coerenza con la normativa vigente, sarà data ai lavoratori adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.
- 5.2. Il trattamento dei dati raccolti avverrà nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza previsti dal Regolamento UE 2016/679, (General Data Protection Regulation).

6. Disposizioni finali

- 6.1. Eventuali modifiche del sistema SmartLocker e dei database sopra citati, derivanti dall'evoluzione tecnologica digitale, che consentano di raggiungere le medesime finalità, saranno oggetto di verifica fra le Parti.
- 6.2. Le Parti condividono l'opportunità di prevedere, trascorsi 12 mesi dalla data di stipula del presente accordo, un incontro di verifica a livello nazionale per monitorare l'avanzamento dell'installazione dei dispositivi, la loro funzionalità nonché gli effetti sul tasso di guasto degli impianti interessati. Su richiesta delle Parti potranno anche essere previsti incontri di verifica a livello territoriale.

Le Parti si danno atto che il presente accordo avente valenza nazionale supera i precedenti accordi stipulati il 26 marzo 2020 nelle regioni Calabria e Toscana aventi un mero carattere sperimentale.

per TIM S.p.A.

per SLC-CGIL

per FISTel-CISL

per UILCOM-UIL

per UGL Telecomunicazioni

per Coordinamento Nazionale RSU