COMUNICAZIONI DA REMOTO: ESIGENZE DI PRIVACY E DI PUBBLICA SICUREZZA

Articolo 75, comma 1, del decreto-legge 17 marzo 2020, n.18, convertito, con modificazioni, dalla legge 24 aprile 2020, n.27

In tema di "*Acquisti per lo sviluppo di sistemi informativi per la diffusione del lavoro agile e di servizi in rete per l'accesso di cittadini e imprese ... le amministrazioni aggiudicatrici ... sono autorizzate, sino al 31 dicembre 2021, ad acquistare beni e servizi informatici, preferibilmente basati sul modello cloud SaaS (software as a service) e, soltanto laddove ricorrono esigenze di sicurezza pubblica ai sensi dell'articolo 4, paragrafo 1, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, con sistemi di conservazione, processamento e gestione dei dati necessariamente localizzati sul territorio nazionale*".

di Giovanni NAZZARO, *Lawful Interception Consultant, Security Manager, Auditor/Lead Auditor* ISO 27001, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da 20 anni, esperto in *security*, *legal* e *compliance* in tali ambiti. Esperto nella progettazione dei sistemi d'intercettazione e di *data retention* e nella definizione delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della "*Lawful Interception Academy*" dal 2014, promotore della *LIA Certification* per la conformità dei sistemi d'intercettazione. E' professore a contratto in Master Universitari di I e II livello.

L'11 marzo 2020 l'OMS ha ufficializzato come "pandemica" la situazione che aveva descritto in precedenza come emergenza di sanità pubblica derivante dalla diffusione del virus covid-19. L'Italia ancor prima, il 31 gennaio 2020, aveva dichiarato uno stato di emergenza generale per sei mesi (fino al 31 luglio 2020) che purtroppo poi è stato prorogato più volte fino ad oggi.
Per far fronte rapidamente all'emergenza il nostro paese è ricorso al decreto-legge come strumento. Sono stati quindi emanati molti decreti, alcuni hanno costituito la base legislativa per l'emanazione dei diversi D.P.C.M. che hanno disciplinato le misure di contenimento e la loro progressiva (e sperata) eliminazione. Altri invece hanno dettato misure per fronteggiare e gestire le emergenze sanitarie, ma soprattutto le conseguenze economiche e sociali derivanti dall'adozione delle misure che, nella pratica, sono andate nella direzione di restringere e ridurre ogni attività, lavorativa ma anche personale.

1. Il decreto-legge "Cura Italia" ed le comunicazioni da remoto

Il Decreto Cura Italia ha cambiato il testo del decreto legge n. 18 del 17 marzo 2020 rubricato "*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*", che è stato il primo provvedimento emanato per rispondere all'emergenza con strumenti economici.
Convertito con modificazioni dalla Legge n. 27/2020, il decreto ha introdotto molte novità:

1) potenziamento delle risorse umane e strumentali del servizio sanitario nazionale;
2) estensione delle misure di carattere fiscale, introdotte inizialmente per la cd. zona rossa di Lombardia e Veneto, a tutto il territorio nazionale;
3) equiparazione del periodo trascorso in quarantena alla malattia;
4) riconoscimento di congedi e vari bonus, tra cui quello per baby sitter;
5) sospensione delle procedure di licenziamento collettivo e dello svolgimento delle procedure concorsuali per l'accesso al pubblico impiego.

La misura più importante, che ha cambiato anche il futuro del modo di lavorare, è rappresentata sicuramente dal ricorso al lavoro agile o c.d. *smart working*, introdotto per qualsiasi rapporto di lavoro subordinato e che ha costituito di fatto la modalità ordinaria di svolgimento della prestazione lavorativa delle pubbliche amministrazioni, oltre a quella del privato, con limitazione della presenza sul posto di lavoro esclusivamente per assicurare attività indifferibili e non altrimenti erogabili.A tal proposito, è proprio nel settore della Giustizia, che più di ogni altro si sono resi evidenti gli effetti del lavoro agile. Vediamo alcuni esempi.

Le misure di distanziamento previste dalla legislazione emergenziale hanno reso difficoltoso a clienti e avvocati incontrarsi per firmare la procura alle liti, quindi è stato introdotto un emendamento affinché la sottoscrizione della procura potesse essere apposta dalla parte anche su un documento cartaceo trasmesso al difensore via email. Nei procedimenti civili innanzi alla Corte di Cassazione il deposito degli atti e dei documenti da parte degli avvocati è stato autorizzato anche in modalità telematica nel rispetto della normativa sulla sottoscrizione, trasmissione e ricezione dei documenti informatici.

Un altro emendamento ha previsto che nel corso delle indagini preliminari il pubblico ministero e il giudice potessero avvalersi di collegamenti da remoto, individuati e regolati con provvedimento del Dgsia, per compiere atti che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone. Il 10 ed il 20 marzo 2020 la Dgsia ha pubblicato due decreti, pressoché simili, che hanno attuato i Decreti Legge n. 11/2020 e 18/2020, prevedendo per le udienze civili (art. 2) e quelle penali (art. 3) l'utilizzo di due soli programmi, entrambi della Microsoft, Skype Business e Teams, specificando che i collegamenti utilizzano infrastrutture dell'amministrazione o aree di *data center* riservate in via esclusiva al Ministero della Giustizia. Il provvedimento della Dgsia non specifica tuttavia la localizzazione geografica (se in Italia oppure altrove) delle aree riservate. Se il riferimento è al cloud, allora i servizi sono forniti tramite i *data center* Microsoft di Dublino e Francoforte, riferimento per l'Europa.
Il problema attuale dei servizi in cloud non è più la sicurezza dei collegamenti da e verso di essi poiché tutti ormai usano protocolli sicuri, piuttosto è quello di comprendere dove risiedono i dati. Queste perplessità sono abbastanza diffuse, tanto che lo stesso Garante della privacy il 16 aprile 2020, quasi 30 giorni dopo il provvedimento della Dgsia, ha scritto di suo pugno una lettera al Ministro della Giustizia

ponendosi seri interrogativi sulle caratteristiche tecniche delle piattaforme indicate dalla Dgsia, nonché sull'opportunità della scelta di un fornitore del servizio in questione stabilito negli Usa e, come tale, soggetto tra l'altro all'applicazione delle norme del **Cloud Act**, "*Clarifying Lawful Overseas Use of Data (Cloud) Act* ", che consente al governo Usa di chiedere ad organizzazioni americane di accedere ai dati ospitati anche su server presenti all'estero.
Il Garante ha lamentato anche l'eccezionalità (ovvero non era mai accaduto prima) con cui l'Autorità non è stata investita di alcuna richiesta di parere sulle norme emanate in merito, con decretazione d'urgenza, né sulle determinazioni della Dgsia in ordine alla scelta della piattaforma e dell'applicativo da indicare, ai fini della celebrazione da remoto del processo penale. Il timore è quali tipologie di dati sono memorizzati da Microsoft per finalità proprie, del servizio o commerciali e sull'eventualità che Microsoft o un amministratore di sistema (anche figura interna all'amministrazione pubblica) possa desumere, dai metadati nella sua disponibilità, alcuni dati "giudiziari" particolarmente delicati quali, ad esempio, la condizione di soggetto sottoposto alle indagini.

2. Le applicazioni SaaS ed il modello di cloud

Un'applicazione che consente una comunicazione da remoto, che può essere un video/audio meeting, oggi è di fatto un'applicazione in cloud. Il paradigma alla base del suo utilizzo è cambiato rispetto al passato, **non si paga più per la licenza ma in base all'utilizzo effettivo ovvero solo per le risorse usate**. Le applicazioni, o meglio i software, così utilizzati in cloud sono indicati con Software as a Service (SaaS) e presentano molti vantaggi:

1) costi ridotti per la configurazione e l'infrastruttura;
2) accessibilità con possibilità di accedere da qualunque parte del modo;
3) scalabilità perché l'utilizzo può essere organizzato per numero di postazioni con accesso e per un tempo prestabilito;
4) aggiornamenti automatici e frequenti;
5) standard di sicurezza comuni a tutti gli utenti, quindi si evita la possibilità che qualche utente possa rappresentare l'anello debole della catena.

Il modello tradizionale del SaaS ha tuttavia degli svantaggi, in parte richiamati proprio nella lettera del Garante della privacy prima citata. Tra tutti probabilmente quello maggiormente sentito è la **cessione dei dati al provider**, ovvero i nostri dati non sono fisicamente in nostro possesso. Questa è la ovvia conseguenza di come sia evoluto il modello di vendita, che è passato da un servizio costoso in cui tutto era in nostro possesso, ad uno economico a discapito però del **possesso del bene più prezioso, i nostri dati**.

Nel caso specifico dei collegamenti da remoto quali potrebbero essere i dati che conserva il cloud provider? Ipotizzando una funzionalità completa di servizi per la comunicazione a distanza, avremmo i dati identificativi dell'utente (username univocamente attribuibili), i dati relativi al chiamante e al chiamato, la durata della conversazione, l'IP utilizzato, i messaggi inviati nella chat di gruppo o personale con i loro allegati (foto, documenti, link, ecc.). Se poi sono presenti altri servizi, come la email oppure il calendario, allora le informazioni sono maggiori, più complesse e con la possibilità anche di correlarle tra loro.

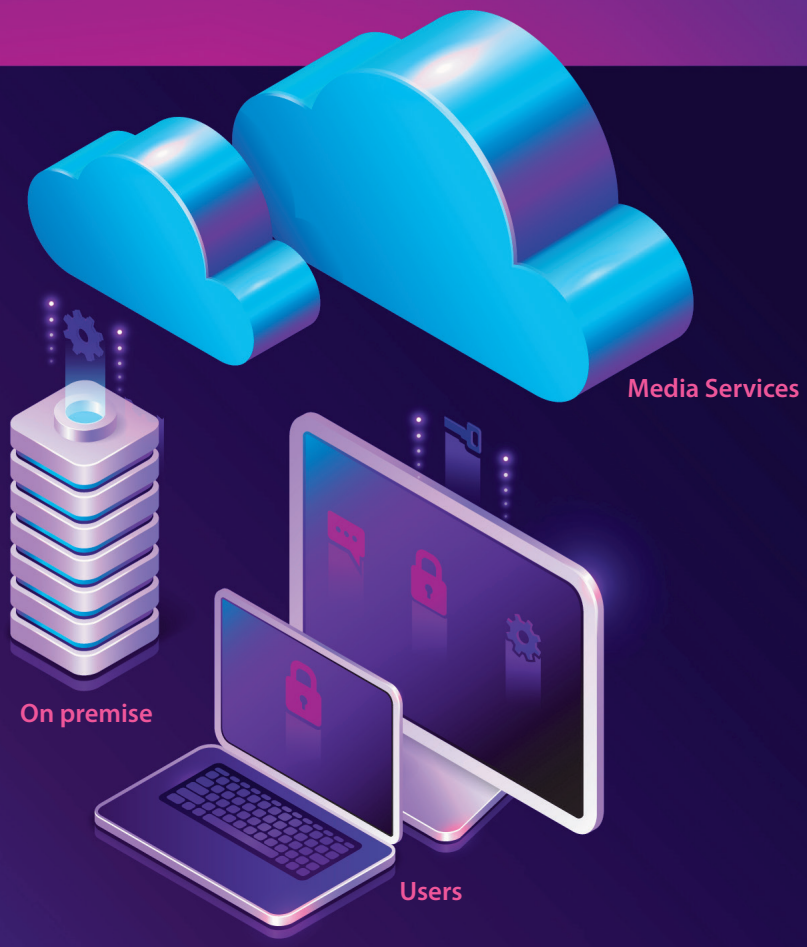
Il servizio fornito per effettuare un collegamento da remoto dipende dal tipo di provider scelto, dal ruolo che svolge nell'erogazione del servizio stesso. In genere le figure coinvolte sono tre:

1) **il provider dell'applicazione**, che è la componente che permette effettivamente di poter stabilire la connessione e di gestire le funzionalità previste, nonché di curare gli aspetti relativi alla privacy e alla sicurezza;
2) **il provider del cloud** o dello spazio fisico dove risiede l'applicazione;
3) **il provider del *media service***, che è la componente che permette esclusivamente di codificare/decodificare il dato affinché sia trasmesso ad esempio per una video chiamata, la cui complessità dipende dal numero di connessioni contemporanee consentite (si pensi ad esempio a meeting con oltre 200 partecipanti).

Fino ad oggi sono esistiti solo due modelli architetturali, quello che segue ancora il vecchio paradigma del pagamento della licenza per avere l'applicazione ed il *media service* in casa, molto costoso, e quello a cui ci si affida ad un unico provider che assume i tre ruoli visti in precedenza, molto economico.

Abbiamo tolto al Cloud
il controllo ed il tracciamento dei tuoi dati

Soluzione per
Video Meeting
realmente sicura



secfull meeting

La prima soluzione hybrid tutta italiana e realmente sicura
per video e audio meeting
con la potenza dei media services in cloud
e i tuoi dati archiviati all'interno della tua organizzazione

Soluzione qualificata AGID
e conforme all'art.75 della L.27/2020
per esigenze di Pubblica Sicurezza.

LEX et ARS

www.secfull.com

info@secfull.com

Scenario	Applicazione	Media service	Vantaggi	Svantaggi	Scala dei costi
Full Cloud	**In cloud**	**In cloud**	Super economico	Dati presso il provider	1
Hybrid	**In casa**	**In cloud**	Dati in casa ed economico	Nessuno	10
Full On premise	**In casa**	**In casa**	Dati in casa	Costoso	100

Infatti, sia l'applicazione che il *media service* si abbinano molto bene con il cloud: un'applicazione può essere su cloud, allora è un SaaS, mentre il *media service* generalmente è sempre su cloud perché quest'ultimo consente di gestire dinamicamente le risorse necessarie.

Oggi però si sta presentando al mercato una terza soluzione, grazie alla presenza di provider che offrono la possibilità di scegliere l'utilizzo separato dello **spazio in cloud** da quello del **media service**, sempre in cloud. Questa nuova soluzione è nata proprio per venire incontro alle sempre più evidenti esigenze stringenti di privacy, quindi ha consentito di riportare in casa la gestione dei propri dati, ma sfruttando le potenzialità del *media service* in cloud e di fatto sollevando le pubbliche amministrazioni e le aziende private da pesanti adeguamenti architetturali e costosi investimenti dovuti all'approvvigionamento di hardware, software e connettività di larga banda richiesti dal tipo di servizio.
Nella tabella in alto abbiamo provato a schematizzare la tipologia di servizio che consente di effettuare comunicazioni da remoto, e che il mercato oggi può offrire, in funzione delle tre figure di provider prima elencate, evidenziandone vantaggi, svantaggi e costi.

3. Pubblica sicurezza e l'art. 75 del Decreto-legge "Cura Italia"

Il Regolamento UE 2018/1807 del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, prevede al "considerando" n.19 la nozione di "**pubblica sicurezza**" come, ai sensi dell'articolo 52 TFUE nell'interpretazione datane dalla Corte di giustizia, **la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati**. Inoltre al considerando n.18 prevede che "è opportuno che gli Stati membri possano invocare unicamente la sicurezza pubblica come giustificazione per gli obblighi di localizzazione dei dati", infatti l'art. 4 comma 1 prevede che "gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità".
L'articolo 75 del decreto-legge "Cura Italia" regola gli "Acquisti per lo sviluppo di sistemi informativi per la diffusione del lavoro agile e di servizi in rete per l'accesso di cittadini e imprese" ed ha disciplinato l'acquisto di beni e servizi informatici, preferibilmente basati sul modello cloud SaaS (software as a service) e, soltanto **laddove ricorrono esigenze di sicurezza pubblica** ai sensi del già ricordato articolo 4, paragrafo 1, del regolamento (UE) 2018/1807, **con sistemi di conservazione, processamento e gestione dei dati necessariamente localizzati sul territorio nazionale, nonché servizi di connettività**.

Come beni e servizi informatici, l'articolo 75 rappresenta una deroga all'obbligo di ricorrere al sistema Consip/Mepa (art. 1, comma 450, legge 27 dicembre 2006, n. 296 e s.s.m.m.- art. 1, commi 510 e 512, Legge 28/12/2015, n. 208), per cercare la soluzione migliore che risponda alle specifiche esigenze della PA. Inoltre, non essendo previsto niente al riguardo, sembra che l'articolo 75 del "Cura Italia" si applichi a contratti di qualunque importo (sopra o sotto le soglie comunitarie).

Il Decreto Milleproroghe del 31 dicembre 2020 ha poi modificato l'articolo 75 del Decreto "Cura Italia", spostando l'autorizzazione ad operare in deroga alle precedenti disposizioni di legge fino al **31 dicembre 2021**. Restano ferme le necessità di rispettare le disposizioni del codice delle leggi antimafia e delle misure di prevenzione della corruzione, nonché di acquisire software presenti nel **marketplace cloud della PA gestito da Agid** (https://cloud.italia.it/marketplace/). ©