CONSIDERAZIONI TECNICHE CIRCA LA PREVISIONE DI "COLLEGAMENTI DA REMOTO" NEL SETTORE PENALE LEGATE ALL'EMERGENZA COVID-19 *

dis CRIMEN opinioni
17.4.2020

Premessa

L'analisi si concentra esclusivamente su alcune criticità tecnico-informatiche, relative all'ampliamento dei casi di collegamento da remoto previsti per la celebrazione di udienze penali e per l'espletamento di atti di indagine nella fase delle indagini preliminari; non sarà qui valutata la compatibilità di tali "innovazioni" con le garanzie costituzionali legate al giusto processo, ma ci si concentrerà unicamente sui problemi relativi alla riservatezza/protezione dei dati ed alla sicurezza informatica delle soluzioni ipotizzate e ipotizzabili.

Riferimenti normativi

È opportuno ricostruire sinteticamente l'*iter* legislativo delle novità introdotte:

- Il primo D.L. "giustizia" 8 marzo 2020, n. 11 all'art. 2, comma settimo (ora già abrogato), amplia le limitate ipotesi di collegamento da remoto previste dall'art. 146-*bis* Disp. Att. c.p.p. estendendo, ove possibile, e sino al 31 maggio p.v., tale modalità di "partecipazione" a qualsiasi udienza, per tutte le persone detenute, internate o in stato di custodia cautelare[1].

* È il testo delle osservazioni tecniche concernenti il c.d. processo a distanza, elaborate dal Centro Studi giuridici sociali "Aldo Marongiu" dell'Unione delle Camere Penali Italiane in collaborazione con l'Avv. Carlo Blengino.

[1] Art. 2 D.L. 11/2020 comma 7: «Ferma l'applicazione dell'articolo 472, comma 3, del codice di procedura penale, a decorrere dal giorno successivo alla data di entrata in vigore del presente decreto e sino alla data del 31 maggio 2020, la partecipazione a qualsiasi udienza delle persone detenute, internate o in stato di custodia cautelare è assicurata, ove possibile, mediante videoconferenze o con collegamenti da remoto individuati e regolati con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia, applicate, in quanto compatibili, le disposizioni di cui ai commi 3, 4 e 5 dell'articolo 146-*bis* del decreto legislativo 28 luglio 1989, n. 271».

Le modalità di tali collegamenti da remoto debbono esser individuate e regolamentate con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia (d'ora innanzi DGSIA).

- Con provvedimento del 10 marzo 2020 il DGSIA dà sintetica attuazione alla delega e all'art. 3[2] prescrive per le udienze penali in principalità l'utilizzo degli strumenti già adottati per i collegamenti di cui all'art. 146-*bis* Disp. Att. a disposizione degli istituti penitenziari e degli uffici giudiziari; o, in alternativa, i programmi attualmente a disposizione dell'Amministrazione – cioè *Skype for Business* e *Teams* – previsti per il settore civile all'art. 2 del medesimo provvedimento. Entrambe le piattaforme indicate dal DGSIA sono piattaforme commerciali di proprietà della *Microsoft Corporation*.

- Con il D.L. 18 del 17 marzo 2020 al comma 12 dell'art. 83[3] viene riproposta, prorogandola sino al 30 giugno p.v., identica previsione di collegamento da remoto per qualsiasi udienza penale, per tutte le persone detenute, internate o sottoposte a misura cautelare, con le medesime modalità di regolamentazione (provvedimento del DGSIA) di cui al precedente Decreto 11/2020, la cui disposizione viene contestualmente abrogata.

- Il DGSIA in attuazione della nuova delega *ex* art. 83, ripropone in data 20 marzo 2020 l'identico sintetico provvedimento di individuazione e regolamentazione: trattandosi di persone detenute, internate o sottoposte a misura cautelare, ove possibile il collegamento dovrà avvenire utilizzando gli strumenti di videoconferenza già a

[2] Provvedimento DGSIA n° 3413 del 10 marzo 2020, art. 3 (Svolgimento delle udienze penali) - «Le udienze penali di cui al settimo comma dell'art. 2 del Decreto-Legge 8 maggio 2020, n. 11, si svolgono, ove possibile, utilizzando gli strumenti di videoconferenza già a disposizione degli uffici giudiziari e degli istituti penitenziari ai sensi dell'art. 146-*bis* del decreto legislativo 28 luglio 1989, n. 271.

In alternativa, possono essere utilizzati i collegamenti da remoto previsti dall'art. 2 del presente provvedimento laddove non sia necessario garantire la fonia riservata tra la persona detenuta, internata o in stato di custodia cautelare ed il suo difensore e qualora il numero degli imputati, che si trovano, a qualsiasi titolo, in stato di detenzione in luoghi diversi, consenta la reciproca visibilità».

[3] «Ferma l'applicazione dell'articolo 472, comma 3, del codice di procedura penale, dal 9 marzo 2020 al 30 giugno 2020, la partecipazione a qualsiasi udienza delle persone detenute, internate o in stato di custodia cautelare è assicurata, ove possibile, mediante videoconferenze o con collegamenti da remoto individuati e regolati con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia, applicate, in quanto compatibili, le disposizioni di cui ai commi 3, 4 e 5 dell'articolo 146-*bis* del decreto legislativo 28 luglio 1989, n. 271».

disposizione degli istituti penitenziari e degli uffici giudiziari per le ipotesi di cui all'art. 146-*bis* Disp. Att.; in alternativa sono riproposti gli applicativi della *Microsoft Skype for Business* e *Teams*.

- In data 9 aprile, in sede di conversione, il Governo pone la fiducia su di un unico emendamento complessivo che introduce notevoli modifiche in relazione all'uso dei collegamenti da remoto nel settore penale. Svincolando l'uso della videoconferenza dallo stato di detenzione del soggetto che dovrebbe "beneficiarne", vengono inseriti all'art. 83 diversi commi volti ad estendere il sistema dei collegamenti da remoto ben oltre le originarie previsioni di cui ai due decreti-legge.

Il collegamento da remoto non è più legato allo stato di detenzione della parte necessaria, ma diviene di fatto regime ordinario "possibile" in udienza per pubblico ministero, parti private e i rispettivi difensori, per gli ausiliari del giudice, gli ufficiali o agenti di polizia giudiziaria, e per gli interpreti, i consulenti o i periti; questo sino al 30 giugno 2020 (comma 12-*bis*)[4].

Il collegamento da remoto diviene inoltre "possibile" anche per atti di indagine nella fase delle indagini preliminari (comma 12-*quater*)[5]; nonché come modalità per

[4] 12-*bis*: «Fermo quanto previsto dal comma 12, dal 9 marzo 2020 al 30 giugno 2020 le udienze penali che non richiedono la partecipazione di soggetti diversi dal pubblico ministero, dalle parti private e dai rispettivi difensori, dagli ausiliari del giudice, da ufficiali o agenti di polizia giudiziaria, da interpreti, consulenti o periti possono essere tenute mediante collegamenti da remoto individuati e regolati con provvedimento del direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Lo svolgimento dell'udienza avviene con modalità idonee a salvaguardare il contraddittorio e l'effettiva partecipazione delle parti. Prima dell'udienza il giudice fa comunicare ai difensori delle parti, al pubblico ministero e agli altri soggetti di cui è prevista la partecipazione, giorno, ora e modalità del collegamento. I difensori attestano l'identità dei soggetti assistiti, i quali, se liberi o sottoposti a misure cautelari diverse dalla custodia in carcere, partecipano all'udienza solo dalla medesima postazione da cui si collega il difensore. In caso di custodia dell'arrestato o del fermato in uno dei luoghi indicati dall'articolo 284, comma 1, del codice di procedura penale, la persona arrestata o fermata e il difensore possono partecipare all'udienza di convalida da remoto anche dal più vicino ufficio della polizia giudiziaria attrezzato per la videoconferenza, quando disponibile. In tal caso, l'identità della persona arrestata o formata è accertata dall'ufficiale di polizia giudiziaria presente. L'ausiliario del giudice partecipa all'udienza dall'ufficio giudiziario e dà atto nel verbale d'udienza delle modalità di collegamento da remoto utilizzate, delle modalità con cui si accerta l'identità dei soggetti partecipanti e di tutte le ulteriori operazioni, nonché dell'impossibilità dei soggetti non presenti fisicamente di sottoscrivere il verbale, ai sensi dell'articolo 137, comma 2, del codice di procedura penale, o di vistarlo, ai sensi dell'articolo 483, comma 1, del codice di procedura penale».

[5] 12-*quater*: «Dal 9 marzo 2020 al 30 giugno 2020, nel corso delle indagini preliminari il pubblico ministero e il giudice possono avvalersi di collegamenti da remoto, individuati e regolati con provvedimento del direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia, per

le deliberazioni collegiali in camera di consiglio per tutti gli organi giurisdizionali, Corte di Assise compresa (comma 12-*quinquies*)[6] e per la Cassazione (comma 12-*ter* che richiama il 12-*quinquies*).

- Al momento il DGSIA non ha ovviamente ancora dato attuazione alle nuove deleghe di cui all'art. 83, previste nella legge di conversione (non ancora in vigore) e dunque non è possibile sapere se riproporrà, per la terza volta, l'identico sintetico provvedimento che designerebbe a questo punto come unico strumento l'utilizzo delle piattaforme *Microsoft Skype for Business* e *Teams*, non risultando più coinvolti nei collegamenti gli istituti di pena e dunque gli strumenti predisposti ai sensi dell'art. 146-*bis* Disp. Att.

Una prima considerazione sulla digitalizzazione forzata

Per comprendere appieno le conseguenze e le problematiche tecniche connesse all'anomala accelerazione della digitalizzazione del processo penale nell'emergenza, che

compiere atti che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone, nei casi in cui la presenza fisica di costoro non può essere assicurata senza mettere a rischio le esigenze di contenimento della diffusione del virus COVID-19. La partecipazione delle persone detenute, internate o in stato di custodia cautelare è assicurata con le modalità di cui al comma 12. Le persone chiamate a partecipare all'atto sono tempestivamente invitate a presentarsi presso il più vicino ufficio di polizia giudiziaria, che abbia in dotazione strumenti idonei ad assicurare il collegamento da remoto. Presso tale ufficio le persone partecipano al compimento dell'atto in presenza di un ufficiale o agente di polizia giudiziaria, che procede alla loro identificazione. Il compimento dell'atto avviene con modalità idonee a salvaguardarne, ove necessario, la segretezza e ad assicurare la possibilità per la persona sottoposta alle indagini di consultarsi riservatamente con il proprio difensore. Il difensore partecipa da remoto mediante collegamento dallo studio legale, salvo che decida di essere presente nel luogo ove si trova il suo assistito. Il pubblico ufficiale che redige il verbale dà atto nello stesso delle modalità di collegamento da remoto utilizzate, delle modalità con cui si accerta l'identità dei soggetti partecipanti e di tutte le ulteriori operazioni, nonché dell'impossibilità dei soggetti non presenti fisicamente di sottoscrivere il verbale, ai sensi dell'articolo 137, comma 2, del codice di procedura penale».

[6] 12-*quinquies*: «Dal 9 marzo 2020 al 30 giugno 2020, nei procedimenti civili e penali non sospesi, le deliberazioni collegiali in camera di consiglio possono essere assunte mediante collegamenti da remoto individuati e regolati con provvedimento del direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Il luogo da cui si collegano i magistrati è considerato camera di consiglio a tutti gli effetti di legge. Nei procedimenti penali, dopo la deliberazione, il presidente del collegio o il componente del collegio da lui delegato sottoscrive il dispositivo della sentenza o l'ordinanza e il provvedimento è depositato in cancelleria ai fini dell'inserimento nel fascicolo il prima possibile e, in ogni caso, immediatamente dopo la cessazione dell'emergenza sanitaria».

giunge con un balzo sino alla virtualizzazione del rapporto processuale e alla creazione di atti di indagine in remoto, sarebbe invero necessario ripercorrere la travagliata storia della digitalizzazione della Pubblica Amministrazione italiana e quella altrettanto sofferta dell'applicabilità dei principi dettati dal CAD (Codice dell'Amministrazione Digitale D.Lvo 82/2005) all'attività giudiziaria e in particolare al processo penale.

Ai fini di queste note è però opportuno limitarsi a sottolineare come la lenta progressione del c.d. PPT, ovvero del Processo Penale Telematico, rispetto al più avanzato PCT, il Processo Civile Telematico, ha trovato da sempre fondate ragioni nelle caratteristiche peculiari della giustizia penale, prime fra tutte le stringenti garanzie costituzionali che caratterizzano la giurisdizione penale e i ben noti vincoli di segretezza e riservatezza.

Se nel processo penale è (era) impossibile anche solo depositare telematicamente a mezzo PEC una banale istanza di interrogatorio, ciò non è da attribuirsi ad una particolare ottusità del settore penale, ma alla delicatezza di un sistema che deve garantire principi costituzionali fondamentali e livelli di sicurezza/riservatezza del tutto peculiari.

Il mondo digitale e l'infosfera che si genera con l'utilizzo delle reti di comunicazione crea un ambiente virtuale di difficile governo, fragile e vulnerabile, ed ogni innovazione tecnologica impone sempre (*ex lege* come vedremo) una valutazione d'impatto complessa, che rivela spesso rischi inaspettati su diritti, in generale e nel processo penale in particolare, tutt'altro che virtuali.

È singolare dunque che, improvvisamente, con l'emergenza, tutto diventi possibile, nel bene e nel male: si scopre che la R.U.G. (la Rete Unica Giustizia) non è quel baluardo impenetrabile da parte degli avvocati e che i depositi telematici a mezzo P.E.C. si possono fare anche nel settore penale (bene!) e si decide che delicati atti che sono al cuore della giustizia penale, come un interrogatorio o un dibattimento, si possono compiere attraverso banali applicativi commerciali come *Skype for Business* e *Teams*, sulla rete pubblica internet (malissimo!)[7].

Verrebbe da pensare, delle due l'una: o per un'inspiegabile e malcelata insofferenza verso i fruitori del servizio fino ad ora il procedimento penale ha costretto i suoi utenti a pratiche desuete e inutili, come i depositi cartacei in cancelleria o l'accesso ai fascicoli con defatiganti procedure di copia (fotostatica o informatica) direttamente

[7] La connessione del difensore da remoto è già prevista da alcune Autorità Giudiziarie per le direttissime (cfr: *http://ordineavvocati.padova.it/wp-content/uploads/2020/03/vademecum-protocollo-direttissime.pdf*).

presso gli uffici giudiziari; oppure una ragione c'era, fondata e insita nella peculiarità della giurisdizione penale e nella complessità delle tecnologie digitali, ed allora è difficile comprendere come tali ragioni siano improvvisamente sparite grazie al virus.

Ciò osservato, al momento non è dato sapere come il DGSIA intenda attuare la delega tecnica conferita dal nuovo art. 83 del D.L. 18/2020 che come visto prevede la facoltà di collegamento da remoto indipendentemente dalla condizione di detenzione del soggetto virtualizzato.

In realtà, prima delle improvvide modifiche in sede di conversione, il fatto che il soggetto in collegamento fosse in stato di detenzione dava la possibilità di utilizzare gli applicativi già testati nella precedente disciplina prevista dall'art. 146-*bis* Disp. Att. ed inoltre gli istituti di detenzione davano garanzia di verifica dei collegamenti utilizzati, che avvenivano tra postazioni e *client* "ufficiali" della Pubblica amministrazione. L'ampliamento del collegamento remoto a molteplici soggetti esterni, dall'avvocato all'imputato libero sino all'ufficiale di P.G. e al magistrato stesso in camera di consiglio, che ovviamente debbono potersi collegare tramite internet da postazioni o dispositivi privati, con *client* o interfacce *web* di uso gratuito, pone problemi inediti tanto in tema di sicurezza (*cyber security*) quanto in tema di trattamento dei dati generati sulla rete.

Pensare di utilizzare per detti collegamenti tra *client* esterni alla R.U.G., applicativi commerciali quali *Microsoft Skype for Business* e *Microsoft Teams*, ovvero le due piattaforme ad oggi individuate dal DGSIA, appare un azzardo e non consente di rispettare le garanzie minime di sicurezza, riservatezza e protezione dati richieste dalla normativa.

Prima di analizzare i predetti applicativi *software*, è necessario un breve accenno alla normativa di settore.

Il Decreto Legislativo 18 maggio 2018, n. 51 di attuazione della direttiva (UE) 2016/680

La direttiva (UE) 2016/680 del 27 aprile 2016, "*relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*" è stata emanata proprio per garantire che, con l'evoluzione tecnologica, anche l'attività di indagine, accertamento e perseguimento dei reati da parte della magistratura e delle forze dell'ordine sia svolta nel pieno rispetto del diritto

alla protezione del dato, che è uno degli aspetti fondanti della riservatezza e della sicurezza in rete.

È del tutto evidente che l'utilizzo di *software* proprietari e di piattaforme commerciali *cloud* per la realizzazione di collegamenti da remoto nelle udienze e negli atti di indagine implica necessariamente il trattamento, da parte di più soggetti e con diversi ruoli, di molteplici dati personali, alcuni dei quali potenzialmente rientranti tra le categorie di dati particolari (un tempo denominati dati sensibili) di cui all'art. 7 del D.L.vo 51/18.

Nell'introdurre una nuova tecnologia all'interno delle finalità di indagine ed accertamento, il Decreto Legislativo 58/2018 che attua la Direttiva 680/90 richiede al Titolare del trattamento, ovvero l'autorità competente (art. 2 lett. h), precisi obblighi:

Art. 15

Obblighi del titolare del trattamento

1. Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del presente decreto.

Non solo.

Art. 23

Valutazione d'impatto sulla protezione dei dati

1. Se il trattamento, per l'uso di nuove tecnologie e per la sua natura, per l'ambito di applicazione, per il contesto e per le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali.

2. La valutazione di cui al comma 1 contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto.

È lecito dubitare che tali valutazioni siano state fatte (o siano in corso) per gli specifici trattamenti introdotti dai nuovi decreti, ma in ogni caso sarebbe da chiederne copia al DGSIA. È fondamentale sapere se il servizio avvenga attraverso *server* dedicati

o con tecnologia *p2p*, quali dati si genereranno ad ogni connessione a *Teams*, su quali dispositivi sarà conservata traccia delle sessioni in remoto, quali dati permarranno e quali utilizzi farà il *provider* di tali dati (che nel caso di *Microsoft* è tra l'altro un *provider* straniero) e che tipo di misure di sicurezza siano previsti nei termini di servizio.

In realtà queste sono soltanto alcune delle possibili criticità di un'operazione quale quella in atto, di digitalizzazione forzata del processo penale, di cui è difficile fare una chiara valutazione non essendo noti allo stato né la (probabile) scelta degli applicativi (presumibilmente quelli di *Microsoft* già indicati nei precedenti provvedimenti), né soprattutto quale tipo di licenza e quali Termini di Servizio leghino il Ministero della Giustizia alla società di Redmond (Stati Uniti) e quali siano le specifiche tecniche del servizio.

Microsoft Corporation come nodo nell'amministrazione della giustizia italiana.

Descrivere *Skype for Business* e *Microsoft Team*, ovvero i due potenziali applicativi per i futuri collegamenti, è piuttosto complesso.

Il primo è sostanzialmente la versione commerciale del noto *software Skype*, oggi di proprietà di *Microsoft*, che con tecnologia proprietaria *peer to peer* consente comunicazioni audio-video sulla rete internet. Il secondo, *Teams*, è parte di una complessa piattaforma che racchiude in sé decine di funzionalità ed è legata al pacchetto di applicativi *Office 360* sempre di *Microsoft*. Di fatto, *Teams* è l'evoluzione di *Skype for Business* all'interno di una piattaforma di comunicazione e gestione documentale in *cloud* per il mondo business.

Il concorrente diretto di *Microsoft Teams* è *Google Suite* (più nota al grande pubblico), le cui funzionalità sono molto simili. Dunque, dati fondamentali del procedimento penale saranno trattati, ed anzi generati, da *Microsoft* sui propri *server*, attraverso la rete internet. Fosse *Google* farebbe più effetto dirlo, ma il risultato è identico.

Microsoft è fornitore del Ministero della Giustizia da tempo (approssimativamente dal 2007) e *Office 360* (ovvero la suite madre di *Teams*) è parte del "Sistema per la Redazione Atti e Documenti", che a sua volta è un modulo applicativo del S.i.c.p. (Sistema Informativo della Cognizione Penale) .

Purtroppo, per la redazione delle presenti osservazioni non è stato possibile risalire a quale tipo di licenza sia legata la fornitura all'autorità giudiziaria italiana dei

prodotti *Microsoft*, né quali siano i Termini del servizio che intercorrono tra *Microsoft Corporation* e il Ministero della Giustizia.

Microsoft offre commercialmente molteplici livelli di accesso alle proprie tecnologie, tutte rigorosamente proprietarie e dunque segrete, ed è difficile fare una analisi dei possibili rischi in termini di sicurezza e protezione dati senza adeguata documentazione.

È proprio per evitare queste opacità, che rischiano di compromettere la trasparenza del sistema digitale in punti vitali dell'attività dello Stato, che il C.A.D. all'art. 68 "analisi comparativa delle soluzioni"[8] predilige i *software open source* aperti.

L'unico documento che si è potuto reperire è la circolare prot. n. m_dg.DOG. 07.25022020.0007048.U "Diffusione licenze *Microsoft Office* per il personale in servizio presso il Ministero della giustizia e gli Uffici giudiziari" da cui sembrerebbe dedursi che l'applicativo *Teams* sia legato ad una licenza *Office 365 E1*, ma è elemento troppo labile per poter valutare tecnicamente i livelli di sicurezza e di compliance.

Verificabile – invece – da chiunque è il funzionamento di *Teams* e di *Skype* da parte degli utenti privati; tali sarebbero gli avvocati e i vari soggetti costretti a collegarsi da remoto alle stanze virtuali dei magistrati. Basta scorrere l'informativa *privacy* dei due servizi per capire che tali applicativi *free* sono totalmente inadatti ad un utilizzo professionale, men che mai per attività processuali, da parte di chicchessia.

Un' ultima annotazione è opportuna: ad aprile del 2019 è stata aperta una indagine del EDPS (*European Data Protection Supervisor*), il Garante Europeo, proprio in relazione a diverse criticità emerse nei rapporti contrattuali tra *Microsoft Corporation* e diverse istituzioni e organi europei sui servizi *Office360Plus*. L'indagine era ancora in corso al 19 ottobre scorso ed aveva rilevato evidenti carenze in relazione proprio alla normativa a protezione dei dati[9].

[8] Art. 68 C.A.D. D.L.vo 82/2005: «1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: a) *software* sviluppato per conto della pubblica amministrazione; b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione; c) **software libero o a codice sorgente aperto;** d) *software* fruibile in modalità cloud computing; e) *software* di tipo proprietario mediante ricorso a licenza d'uso; f) *software* combinazione delle precedenti soluzioni...».

[9] Si vedano i due comunicati dell'EDPS reperibili qui: *https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements_en*;

e qui: *https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en*;

In Germania Michael Ronellenfitsch, il *Data Protection Officer* (Dpo) dello Stato dell'Assia, ha vietato il *cloud* di *Microsoft* dalle scuole dello stato federato, dichiarando: "*Microsoft Office 365 non dovrebbe essere utilizzato nelle scuole a causa di problemi di privacy per studenti e docenti, perché, anche se i server sono in Europa, per effetto del Cloud Act di Trump i dati possono essere trasmessi all'intelligence Usa. Occorre garantire la sovranità digitale sui dati della P.A.*".

Ovviamente per affermare che i servizi *cloud* offerti al Ministero soffrano di identiche falle di sicurezza è necessario sapere quale tipo di licenza e quale sia il livello di sicurezza garantito nelle TOS (*terms of service*) sottoscritti con *Microsoft*.

Restano in ogni caso insormontabili almeno due problemi: i) il *provider* del servizio, *Microsoft*, è comunque una società americana, sottoposta agli obblighi (ed alle pressioni) dei governi e delle agenzie del proprio paese: il *Cloud Act* voluto da Trump nel 2018 impone ai *provider* americani la *discovery* dei dati alle Autorità statunitensi anche se detenuti in Europa; ii) al di là degli accordi contrattuali in atto, permane il problema insormontabile dei collegamenti "privati", necessariamente effettuati da soggetti esterni alla R.U.G. (gli avvocati *in primis*), tramite rete pubblica con interfacce (applicativi locali o *web*) del tutto inadeguate ad un uso professionale.

CONCLUSIONI

Le soluzioni proposte sino ad ora dal DGSIA appaiono (per quanto noto) inaccettabili e contrastano con l'attuale specifica normativa a protezione dei dati e con le basi stesse della sicurezza informatica in un settore delicato quale la giurisdizione penale.

È necessario inoltrare formale richiesta al Ministero di Giustizia ed al DGSIA per conoscere le caratteristiche e le specifiche tecniche degli applicativi individuati (e individuandi) dal DGSIA in attuazione dell'art. 83 D.L. 18/20 come modificato in sede di conversione e richiedere al Ministero ogni documentazione circa i rapporti contrattuali delle forniture di *Skype for Business* e *Teams*.

È necessario avere accesso alla valutazione d'impatto sulla protezione dei dati svolta *ex* art. 23 D.L.vo 51/18 (se esistente) in relazione allo specifico e inedito servizio di remotizzazione di atti e udienze nel settore del processo penale.

nonché: *https://www.corrierecomunicazioni.it/privacy/gdpr-il-garante-ue-seri-dubbi-sulla-compliance-dei-contratti-microsoft/.*

È opportuno fare una segnalazione al Garante, affinché sia valutato il rispetto della normativa di cui al D.L.vo 51/2018 nelle soluzioni tecnologiche individuate dal Ministero per la "virtualizzazione" di atti e udienze penali.

* * *

Il Processo Penale Telematico non è di fatto mai iniziato, per una serie di problematiche insite nelle peculiarità della giurisdizione penale.

Tecnicamente, a differenza che nel PCT, il settore della giustizia penale è caratterizzato tra l'altro da applicativi diversi per le varie funzioni, da molteplici banche dati non sempre compatibili tra loro e da una totale chiusura della Rete Unica Giustizia (R.U.G.), inaccessibile dall'esterno. Queste particolarità, a torto o a ragione, hanno impedito innovazioni anche banali che avrebbero velocizzato il processo e, nella presente emergenza, evitato accessi fisici agli uffici: si pensi ai depositi telematici da parte degli avvocati (ora realizzati a mezzo PEC senza per la verità alcuna valutazione di compatibilità con il CAD) o alla predisposizione di accessi da remoto a "veri" fascicoli processuali in formato elettronico (che non sono ovviamente la brutale scansione in formato pdf immagine di interi faldoni, con file ingestibili, come avviene in quasi tutte le Procure della Repubblica).

Molto si può fare per usare la tecnologia nelle aule penali.

Ciò detto, al di là di ogni valutazione circa la dubbia compatibilità di udienze e atti "virtuali" con i principi costituzionali legati al giusto processo, l'Amministrazione della Giustizia deve prendere atto che allo stato **nessun fornitore di servizi commerciali è in grado di garantire il rispetto delle stringenti normative tecniche vigenti (dal CAD al GDPR sino alla *Police Directive* di cui al D.L.vo 51/18) nella predisposizione di udienze e atti di indagine da remoto nel processo penale.**

Gli applicativi *Teams* e *Skype* sono tra i migliori sul mercato quanto a resa e sicurezza, ma sono totalmente inadatti alla funzione che gli si vorrebbe assegnare. Sono prodotti commerciali, pensati per imprese commerciali, che offrono mille funzionalità e mille interfacce molto "sexy" e molto "*smart*": ognuna di queste funzionalità è un punto di debolezza per la sicurezza e la protezione dei dati e genera unicamente criticità in un ambiente protetto e "particolare" qual è un processo penale.

Da un punto di vista informatico solo un applicativo *open source* sviluppato *in house* con un'architettura forte calibrata *by design* sul processo penale, appoggiato su

server propri del Ministero e con collegamenti protetti, potrebbe forse rispondere alle esigenze sottostanti le innovazioni portate dal d.d.l. di conversione del D.L. 18/20.

Ci sembra dunque decisamente più agevole prevedere cautele "analogiche" come mascherine, aule grandi per il distanziamento e orari scaglionati piuttosto che innamorarsi della prima soluzione tecnologica disponibile sul mercato.