GIUSTIZIA INSIEME

Diritto e Processo Amministrativo

“Fare (dello stato) di necessità, virtù”. Il decreto Pres. Cons. Stato n. 134/2020 visto dal Garante della privacy

di Piergiuseppe Otranto

28 maggio 2020

ABSTRACT

Warning: Undefined array key "abstract" in **/var/www/vhosts/giustiziainsieme.it/httpdocs/print/articolo_pdf.php** on line **334**

Warning: Undefined array key "sommario_indice" in /var/www/vhosts/giustiziainsieme.it/httpdocs/print/articolo_pdf.php on line 335

"Fare (dello stato) di necessità, virtù”. Il decreto Pres. Cons. Stato n. 134/2020 visto dal Garante della privacy

di Piergiuseppe Otranto

Sommario: 1. Premessa. - 2. Il quadro normativo di riferimento. - 3. L’ “udienza da remoto” e la piattaforma prescelta. - 4. Il consenso al trattamento dei dati personali. - 5. Il *digital divide* cognitivo. - 6. Considerazioni di sintesi.

1. Premessa

Il 22 maggio 2020 il Presidente del Consiglio di Stato ha adottato il decreto n. 134 recante “regole tecnico-operative per l’attuazione del processo amministrativo telematico, nonché per la sperimentazione e la graduale applicazione dei relativi aggiornamenti”.

In questa sede si svolgeranno alcune considerazioni sulle questioni giuridiche di maggior rilievo che rinvengono dall’analisi del parere – n. 88 del 19 maggio 2020 – reso dal Garante per la protezione dei dati personali sullo schema di decreto.

2. Il quadro normativo di riferimento

L’art. 4, comma 1, del d. l. n. 28 del 30 aprile 2020, ha disposto che nel processo amministrativo, a partire dal 30 maggio e fino al 31 luglio 2020, la trattazione delle cause possa esser svolta non solo in forma “cartolare” (con il deposito di “note di udienza”), ma anche attraverso una discussione orale “mediante collegamento da remoto”[1].

La norma primaria, in particolare, dispone che la trattazione a distanza debba svolgersi secondo modalità idonee a salvaguardare il contraddittorio e l’effettiva partecipazione dei difensori all’udienza e a garantire, altresì, “la sicurezza e la funzionalità del sistema informativo della giustizia amministrativa e dei relativi apparati”.

Il successivo comma 2 rimette ad un decreto del Presidente del Consiglio di Stato l’individuazione delle “regole tecnico-operative per la sperimentazione e la graduale applicazione degli aggiornamenti del processo amministrativo telematico”, ma “nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente” [2].

La norma primaria, tuttavia, – ed è questo un profilo che meriterebbe un approfondimento adeguato – nella parte in cui affida al Presidente del Consiglio di Stato, la definizione di regole

tecniche che assicurino “il contraddittorio e l’effettiva partecipazione dei difensori all’udienza”, rimette alla valutazione discrezionale dell’organo di vertice della Giustizia amministrativa il compito di determinare regole idonee ad incidere su aspetti fondamentali delle garanzie previste *ex* artt. 24 e 111 Cost. e sulla stessa riserva di legge in materia processuale.

Le disposizioni di legge, dunque, tracciano un cammino quasi obbligato per i vertici della Giustizia amministrativa: predisporre celermente (ed evidentemente ben prima del 30 maggio) regole tecniche che consentano lo svolgimento del processo da remoto, garantiscano il diritto di difesa ed il contraddittorio oltre che la “sicurezza del sistema”, con la consueta clausola di invarianza finanziaria.

È mancato, in concreto, il tempo sufficiente per approfondire, sotto il profilo tecnico e giuridico, gli effetti delle soluzioni tecnologiche astrattamente configurabili: a partire dal 30 maggio, la trattazione delle cause da remoto costituirà un diritto delle parti del processo con buona pace della gradualità e della attenta ponderazione dei risultati che sono proprie di ogni vera “sperimentazione”.

Il cambio epocale che, senza grande clamore, si introduce nel processo, deve avvenire, poi, in assenza di una dotazione finanziaria adeguata (*recte* di una qualsivoglia dotazione finanziaria).

Un cambio che il legislatore vuole sia implementato, in pochi giorni, con i mezzi e con il personale già a disposizione della giustizia amministrativa.

Un intreccio di obblighi stringenti e ritmi serrati nel quale il Consiglio di Stato – nel dialogo con l’Autorità garante – è stato chiamato a districarsi, individuando una soluzione che, tuttavia, dovrebbe auspicabilmente essere solo temporanea e legata alla situazione emergenziale.

Le considerazioni appena svolte non possono esser trascurate nell’analisi del parere reso sullo schema di decreto dal Garante per la protezione dei dati personali.

3. L’ “udienza da remoto” e la piattaforma prescelta

Il Garante non manca di ricordare che la celebrazione da remoto delle udienze esige una disciplina tecnica fino ad ora non prevista.

In altri termini, non si tratta di migliorare soluzioni tecniche già implementate nell’ambito del processo amministrativo, ma di introdurre in pochi giorni nuove tecnologie e modalità operative per lo svolgimento dell’udienza, per di più senza ulteriori oneri finanziari e nel rispetto di

principi tassativamente indicati.

Tenendosi conto che i dispositivi in dotazione ai magistrati utilizzano il sistema operativo e gli applicativi della *Microsoft*, non sorprende che la scelta sia ricaduta su “*Teams*”[3], applicazione – ricompresa nel pacchetto “Office 365” del colosso di Palo Alto – attraverso cui gli utenti interagiscono online in uno spazio di lavoro ove è possibile condividere file e comunicare attraverso video-chiamate, chiamate vocali, messaggi.

Si tratta, quindi, di un software di tipo “proprietario” del quale non è noto il codice sorgente, cioè quell’insieme di istruzioni tecniche che, scritte in un linguaggio di programmazione, traducono l’algoritmo in una procedura computazionale intellegibile dalla macchina.

La mancata conoscibilità dell’algoritmo e del codice sorgente – sovente protetti come segreti commerciali – rende, così, non pienamente intellegibili e note le operazioni svolte dal software.

Accanto ai programmi a “codice sorgente chiuso”, esistono software *open source* il cui codice sorgente è pubblicato e può, a determinate condizioni, essere studiato, modificato, utilizzato e redistribuito[4].

È evidente che il principio di trasparenza dovrebbe sospingere le Amministrazioni ad utilizzare sempre software *open source*[5] di tal che si possa verificare la conformità al principio di legalità dell’azione realizzata attraverso il programma ed i cittadini possano essere pienamente edotti delle reali modalità di funzionamento di quegli applicativi che sempre più spesso utilizzano dati personali[6] e, da ultimo, finanche adottano (o suggeriscono il contenuto di) decisioni automatizzate[7].

Sotto altro profilo, occorre precisare che l’applicazione *Teams* si regge su una architettura *cloud* e dunque l’archiviazione ed il trattamento dei relativi dati avvengono su *server* controllati da *Microsoft* e non dall’utilizzatore finale[8]. Nel modello c.d. *on premises*, di contro, i dati sono archiviati su infrastrutture gestite o comunque controllate direttamente dal soggetto interessato.

È evidente che la disponibilità e la sicurezza del dato “pubblico” risultano maggiormente garantite da soluzioni *on premises* che, tuttavia, hanno costi notevolmente superiori rispetto a quelle *cloud*.

Sicché, come spesso accade, si registra uno iato tra “ciò che dovrebbe essere” e “ciò che è” e le Amministrazioni utilizzano quasi esclusivamente sistemi operativi e software a codice sorgente chiuso che si reggono su architetture *cloud*, ignare dei possibili effetti pregiudizievoli di tali scelte anche su diritti costituzionalmente garantiti.

Nell’argomentare dell’Autorità questi profili critici appaiono delineati ed immediatamente messi in rilievo.

Ed in vero, nell’*incipit* della parte argomentativa del parere, il Garante auspica che, una volta cessata l’emergenza sanitaria, “si adotti una piattaforma interna, gestita dagli (o sotto lo stretto controllo degli) organi di Giustizia amministrativa. Più in dettaglio, la disponibilità di software *open source* di affidabilità ed accuratezza del tutto comparabili ai migliori prodotti industriali offre il non trascurabile vantaggio di prestarsi a implementazioni di tipo *on premises* (quindi su *datacenter* e reti della Giustizia amministrativa) o comunque su infrastrutture gestite anche collettivamente da o con altre amministrazioni pubbliche”.

Tale auspicio si salda con la condivisibile preoccupazione che l’uso della piattaforma *Microsoft Teams* possa comportare flussi transfrontalieri di dati (anche verso Paesi extra europei)**[9]** in ragione dell’assoggettamento di *Microsoft* alla disciplina statunitense del “Cloud Act”**[10]**.

La legge federale USA, infatti, dispone in capo al prestatore di servizi *cloud* avente sede negli Stati Uniti l’obbligo di copiare e rendere disponibili alle autorità di quel Paese ogni comunicazione elettronica ed ogni altro dato posseduto e relativo ai propri utenti, indipendentemente dal luogo ove tali comunicazioni o dati siano conservati**[11]**.

Secondo il Garante, il rischio che le autorità USA realizzino un trattamento di dati personali non conforme alla disciplina europea sarebbe limitato alle informazioni relative all’identità delle parti coinvolte nell’udienza che verrebbero registrate nei “sistemi di autenticazione *Microsoft* e poi conservat[e] per finalità e per tempi previsti nelle privacy policy aziendali”**[12]**.

Sembra cogliersi, tuttavia, “in filigrana” il dubbio che anche altri dati relativi allo svolgimento dell’udienza possano essere conservati da *Microsoft* (e quindi esser disponibili per le Autorità nordamericane).

Proprio la natura di software a codice sorgente chiuso, infatti, non consente di avere piena contezza del funzionamento dell’applicazione e, ad esempio, dell’eventuale registrazione della sessione (nel nostro caso coincidente con l’udienza) da parte del proprietario della piattaforma.

Sicché prudentemente il Garante osserva che “*secondo quanto riferito dal Consiglio di Stato*, in assenza di registrazione delle udienze e di scambi di messaggi su chat interna (condivisibilmente esclusi dallo schema di decreto), il provider delle videoconferenze non acquisirebbe alcun dato personale al di fuori dei metadati della videoconferenza (identificativi per l’autenticazione coincidenti con gli indirizzi email, indirizzi IP delle postazioni connesse, data e ora della

connessione)”.

Stante il divieto di registrazione delle udienze (e dell’uso di messaggistica istantanea), sancito dall’art. 2, comma 11 del decreto[13], secondo l’Autorità garante il ricorso al sistema *Microsoft Teams* appare ammissibile “nell’attuale contesto emergenziale”.

Il parere cautamente positivo dell’Autorità si fonda anche sul rilievo per il quale “*invece* le camere di consiglio decisorie [sarebbero] svolte di norma in audioconferenza”.

Il rischio di registrazioni dell’udienza ad opera del gestore della piattaforma (*Microsoft*) aleggia come un “non detto” o, se si vuole, come un rischio “da ignoto tecnologico”, insito nella scelta di utilizzare un sistema proprietario per sua natura opaco.

Sembra, tuttavia, che, nell’argomentare del Garante, il momento della decisione giurisdizionale debba esser assistito da opportune ulteriori cautele se “invece” le camere di consiglio decisorie si svolgono “di norma in audioconferenza”.

A ben vedere, però, il decreto del Presidente del Consiglio di Stato dispone che per la camera di consiglio decisoria possano essere utilizzate in alternativa due distinte modalità: la “*call conference*, attraverso il servizio di audioconferenza, utilizzando gli apparati telefonici in dotazione ai magistrati della Giustizia amministrativa” ovvero una riunione virtuale attraverso la piattaforma *Teams* “con il divieto di utilizzare la messaggistica interna alla piattaforma e la funzione di invio di *file*”[14].

Diversamente da quanto ci si sarebbe potuti attendere dalla lettura del parere, nel decreto non ricorre alcuna indicazione in ordine alla tecnologia preferibile per lo svolgimento delle camere di consiglio decisorie (call conference) essendo la relativa scelta organizzativa rimessa alla discrezionalità dei magistrati.

4. Il consenso al trattamento dei dati personali

L’art. 4, comma 1, d.l. n. 28/2020 dispone che durante l’udienza telematica “si dà atto a verbale delle modalità con cui si accerta l’identità dei soggetti partecipanti e la libera volontà delle parti, anche ai fini della disciplina sulla protezione dei dati”.

Il consenso allo svolgimento dell’udienza da remoto, tuttavia, non può dirsi realmente libero. Ed infatti, in assenza di una piena ed assoluta chiarezza in ordine ai profili sopra richiamati – e relativi al funzionamento della piattaforma, all’archiviazione dei dati generati ed all’uso degli

stessi – la volontà delle parti non è pienamente “libera” (in quanto consapevolmente formata), ma pare piuttosto condizionata da una incolmabile asimmetria informativa.

La “libera volontà delle parti” pare, così, più una fideistica (e quasi inevitabile) adesione all’istanza formulata da un’altra parte o – a più forte ragione – alla decisione del Collegio.

L’opacità del funzionamento della piattaforma, simmetricamente, fa sì che anche l’eventuale opposizione alla discussione da remoto – ammessa dall’art. 4, comma 1, d.l. n. 28/2020, ma solo nei casi in cui la discussione da remoto sia sollecitata su istanza di parte e non quando sia disposta d’ufficio – si possa fondare non già su puntuali ragioni tecniche ma, piuttosto, su argomenti relativi a potenziali violazioni di principi (quali ad esempio il principio di riservatezza dei dati personali, di trasparenza dell’azione amministrativa, di effettività del diritto di difesa, del giusto processo) rilevanti per l’ordinamento nazionale anche alla luce dei beni noti processi di integrazione europea.

Tuttavia, ove si ponga mente alla circostanza che l’ammissibilità della discussione da remoto si fonda su una norma primaria che ha rimesso a un decreto del presidente del Consiglio di Stato l’individuazione delle soluzioni tecniche e, quindi, anche la scelta della piattaforma, può facilmente ipotizzarsi che eventuali (coraggiose, verrebbe da dire) opposizioni fondate sui principi generali siano destinate ad esser disattese.

Sotto altro profilo, l’art. 4, comma 1, del d.l. n. 28/2020 prevede che a verbale sia acquisita una dichiarazione dei partecipanti in relazione alla loro “libera volontà anche ai fini della disciplina sulla protezione dei dati personali”.

A tal proposito il Garante ha osservato che la volontà espressa in relazione allo svolgimento dell’udienza secondo peculiari modalità, “non deve essere sovrapposta con i presupposti di liceità del trattamento che, nel caso di specie, sono rinvenibili negli artt. 6, par. 1, lett. e), 9, par. 2, lett. g), e 10 del G.D.P.R.”**[15]**.

In altri termini, la liceità del trattamento non deriva dalla volontà espressa dall’interessato, ma direttamente dalla necessità di eseguire “un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento” (art. 6, par 1, lett. e) **[16]**.

Secondo il Garante sarebbe stato opportuno che il decreto prevedesse l’informativa sul trattamento dei dati personali contestualmente all’avviso di avvenuto deposito di un’istanza di discussione da remoto (art. 2, comma 3 del decreto) “al fine di consentire alle parti una

consapevole valutazione anche sotto il profilo della protezione dati, in ordine alla scelta sull’opportunità di presentare o meno opposizione”.

Tale suggerimento non è stato recepito, sicché l’avvertimento che la celebrazione dell’udienza da remoto comporta il trattamento dei dati personali “anche da parte del gestore della piattaforma” viene formulato nella comunicazione di fissazione dell’udienza (art. 2, comma 5), che comunque precede il momento in cui l’interessato effettivamente si autentica su *Teams*.

Anche sotto il profilo sostanziale, qualora l’informativa (*ex* artt. 13 e 14 G.D.P.R.) sul trattamento dei dati nelle udienze da remoto fosse già presente sul sito della Giustizia amministrativa (e dunque consultabile liberamente finanche prima dell’invio dell’avviso di avvenuto deposito *ex* comma 3), non pare che l’attuale disciplina comporterebbe un pregiudizio significativo per gli interessati.

5. Il *digital divide* cognitivo

Nel parere si sottolinea la necessità di utilizzare correttamente il sistema per evitare che possano prender parte alle udienze soggetti non autorizzati, quali ad esempio soggetti che abbiano titolo per partecipare a udienze precedenti o successive.

In proposito, l’art. 3, comma 4, dell’allegato 3 al decreto dispone che tutti coloro che vengono ammessi a partecipare a un collegamento da remoto in videoconferenza “terminata la discussione della causa (…) non abbandonano la riunione virtuale in autonomia, ma attendono di esserne rimossi”. Sembra, dunque, che spetti all’ufficio curare tanto l’ammissione alla riunione virtuale, quanto la rimozione dalla stessa, sicché appare particolarmente opportuno l’invito dell’Autorità a adottare iniziative volte alla formazione del personale.

Ma anche sul punto la clausola di invarianza finanziaria finisce per attribuire ai vertici degli uffici della Giustizia amministrativa l’arduo compito di rinvenire nelle pieghe dei bilanci i fondi necessari a realizzare adeguati percorsi formativi a beneficio del personale.

Il *digital divide* cognitivo, infatti, come quello infrastrutturale, costituisce un ostacolo significativo per un uso efficace e consapevole delle tecnologie.

Con sempre maggior frequenza l’esercizio di diritti fondamentali, anche costituzionalmente garantiti, presuppone l’uso esclusivo della rete internet e di software specifici. Tali diritti possono essere in concreto esercitati solo qualora esista un’infrastruttura di telecomunicazione diffusa ed

efficiente e qualora gli interessati non solo abbiano dispositivi hardware compatibili con i software utilizzati, ma siano in possesso di competenze culturali adeguate.

Sulla scorta del dettato dell’art. 97 Cost. e delle riflessioni anche risalenti della dottrina amministrativistica, per tal via il profilo dell’organizzazione amministrativa si salda con quello dell’azione, in un disegno finalizzato all’imparzialità e al buon andamento dei pubblici poteri.

Diviene, così, ineludibile un vasto programma di formazione (almeno) del personale pubblico, onde conseguire la piena ed effettiva attuazione dei diritti di cittadinanza digitale in particolare, nel caso che ci occupa, del diritto di difesa innanzi al Giudice amministrativo in un processo nel quale vivano pienamente le regole del contraddittorio, con le opportune garanzie di riservatezza.

Nella prospettiva del necessario superamento del *digital divide* cognitivo non pare convincente la disposizione dell’art. 3, comma 4, dell’allegato 3 al decreto ove si afferma che “la Giustizia amministrativa non fornisce alcuna assistenza tecnica ai soggetti ad essa estranei che partecipano alle udienze e, pertanto, spetta ad essi la preventiva verifica della funzionalità del collegamento telematico dalla propria sede”.

Si è ben consapevoli del carico di lavoro che grava gli uffici della Giustizia amministrativa. Pur tuttavia, considerata la repentina introduzione della disciplina dell’udienza “da remoto”, sarebbe auspicabile almeno la predisposizione di linee guida o tutorial a beneficio dei soggetti (diversi dai magistrati) chiamati a partecipare al “nuovo” processo amministrativo.

Superato il periodo emergenziale, dovranno esser realizzate – anche d’intesa con le associazioni che rappresentano l’avvocatura – opportune iniziative di formazione, per evitare che, dal processo amministrativo telematico e in particolare dalle udienze da remoto, restino di fatto esclusi avvocati che – magari solo per ragioni anagrafiche o per una certa avversione alle tecnologie – non abbiano una sufficiente dimestichezza con i nuovi applicativi ma che, non di meno, sono portatori di un sapere del quale, attraverso un proficuo scambio di vedute, da sempre si alimenta la stessa giurisdizione.

6. Considerazioni di sintesi

Come si è osservato, dal decreto del Presidente del Consiglio di Stato emergono numerosi profili critici meritevoli di quella ponderazione e quell’approfondimento tecnico-giuridico che, nelle condizioni date, è stato possibile svolgere solo parzialmente.

Anzitutto occorrerà riflettere sulla legittimità costituzionale della scelta operata dal legislatore di rimettere ad un atto regolamentare la definizione di aspetti che, attraverso norme di carattere tecnico, sono idonei a incidere su diritti fondamentali, sovente coperti da riserva di legge, come nel caso del principio del giusto processo.

In considerazione, tuttavia, dell’esiguo tempo a disposizione e della clausola di invarianza finanziaria che sovrastano tutto il disegno riformatore del processo amministrativo prefigurato dal legislatore, i vertici della Giustizia amministrativa hanno assolto al compito affidato attraverso soluzioni che, in una situazione emergenziale – e non oltre – paiono accettabili.

D’altra parte, l’esigenza ineludibile di una risposta di carattere emergenziale dell’ordinamento in presenza di eventi straordinari trova fondamento anche nelle riflessioni teoriche sullo “stato di necessità” come fonte del diritto sviluppate sin da epoca anteriore all’introduzione della disciplina positiva della decretazione d’urgenza**[17]**.

Consapevole del proprio ruolo di garante di diritti fondamentali del cittadino ma, non di meno, di Autorità che opera nell’ordinamento generale e che – sempre nell’osservanza della legge – alle repentine evoluzioni dello stesso è chiamata ad adattarsi, il Garante per la protezione dei dati personali ha reso un parere nel quale adombra appena i profili più problematici della disciplina regolamentare introdotta, lasciando chiaramente intendere, tuttavia, che il proprio giudizio (che può dirsi cautamente positivo) trova un solido fondamento nell’esigenza, unitariamente avvertita dall’ordinamento, di far fronte all’emergenza sanitaria.

Le indicazioni di maggior rilievo, per tale ragione, si colgono nel riferimento ottativo alle azioni da porre in essere allorquando la situazione emergenziale sarà cessata: l’ordinamento dovrà dotarsi di regole che prevedano l’utilizzo di software *open source* e che siano fondati su *data center* e reti gestiti direttamente dalla Giustizia amministrativa o comunque da pubbliche amministrazioni, abbandonando soluzioni che, cessata l’emergenza, parrebbero di dubbia legittimità.

Non resta che auspicare che, per allora, il legislatore non chiami il sistema della Giustizia amministrativa (e, *in parte qua*, l’avvocatura) ad affrontare in solitudine la transizione epocale verso il “processo da remoto”, lasciandolo sguarnito di uomini e di mezzi adeguati alla complessità dell’obiettivo perseguito.

[1] “A decorrere dal 30 maggio e fino al 31 luglio 2020 può essere chiesta discussione orale con istanza depositata entro il termine per il deposito delle memorie di replica ovvero, per gli affari cautelari, fino a cinque giorni liberi prima dell’udienza in qualunque rito, mediante

collegamento da remoto con modalità idonee a salvaguardare il contraddittorio e l’effettiva partecipazione dei difensori all’udienza, assicurando in ogni caso la sicurezza e la funzionalità del sistema informatico della giustizia amministrativa e dei relativi apparati e comunque nei limiti delle risorse attualmente assegnate ai singoli uffici. L’istanza è accolta dal presidente del collegio se presentata congiuntamente da tutte le parti costituite. Negli altri casi, il presidente del collegio valuta l’istanza, anche sulla base delle eventuali opposizioni espresse dalle altre parti alla discussione da remoto. Se il presidente ritiene necessaria, anche in assenza di istanza di parte, la discussione della causa con modalità da remoto, la dispone con decreto. In tutti i casi in cui sia disposta la discussione da remoto, la segreteria comunica, almeno un giorno prima della trattazione, l’avviso dell’ora e delle modalità di collegamento. Si dà atto a verbale delle modalità con cui si accerta l’identità dei soggetti partecipanti e la libera volontà delle parti, anche ai fini della disciplina sulla protezione dei dati personali. Il luogo da cui si collegano i magistrati, gli avvocati e il personale addetto è considerato udienza a tutti gli effetti di legge. In alternativa alla discussione possono essere depositate note di udienza fino alle ore 9 antimeridiane del giorno dell’udienza stessa o richiesta di passaggio in decisione e il difensore che deposita tali note o tale richiesta è considerato presente a ogni effetto in udienza. Il decreto di cui al comma 2 stabilisce i tempi massimi di discussione e replica”.

[2] L’art. 4, comma 2, del d. l. n. 28 del 30 aprile 2020, ha sostituito l’art. 13, comma 1, dell’allegato 2 al d.lgs. 2 luglio 2010, n. 104, disponendo: “Con decreto del Presidente del Consiglio di Stato, sentiti il Dipartimento della Presidenza del Consiglio dei ministri competente in materia di trasformazione digitale e gli altri soggetti indicati dalla legge (…) sono stabilite, nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, le regole tecnico-operative per la sperimentazione e la graduale applicazione degli aggiornamenti del processo amministrativo telematico”.

[3] Art. 2, comma 2, lett. b dell’allegato 3 al decreto.

[4] Secondo Corte cost., sentenza 26 marzo 2010, n. 122 in *Foro it.*, 2010, I, 2650, «un programma open source è un software che il *creatore* ha deciso di mettere a disposizione degli altri utenti, autorizzandoli a studiare il codice sorgente, a modificarlo e a ridistribuirlo liberamente, sia pure con le limitazioni che le parti possono pattuire nell’ambito dell’autonomia negoziale».

[5] La propensione dell’ordinamento verso l’uso di software aperto da parte dell’Amministrazione emerge, ad esempio, dalla disciplina dettata dagli artt. 68 e 69 del d.lgs. 7 marzo 2005, n. 82. Si tratta, tuttavia, di una propensione più declamata che effettivamente

praticata, come emerge, tra l’altro, anche dalla vicenda della quale ci stiamo occupando.

[6] Il 25 maggio 2020, ad esempio, è stato pubblicato il codice sorgente della *app* “Immuni”, sistema di notifica delle esposizioni al virus Covid-19.

[7] Secondo Cons. St., sez. VI, 13 dicembre 2019, in caso di decisione amministrativa automatizzata la “conoscibilità dell’algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che i criteri, i presupposti e gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato”.

[8] L’art. 3, comma 3, dell’allegato 3 al decreto precisa che la piattaforma *Teams* “ a) assicura il rispetto della sicurezza delle comunicazioni attraverso avanzati sistemi di crittografia del traffico dati; b) prevede, per gli utenti interni all’amministrazione, l’autenticazione centralizzata a livello di organizzazione e la crittografia dei dati in transito e a riposo; c) utilizza *data center* localizzati sul territorio dell’Unione europea, nei quali vengono conservati e trattati i dati raccolti per l’erogazione del servizio; d) procede al trattamento dei dati personali nel rispetto delle disposizioni del Regolamento (UE) 2016/679”.

[9] Sul punto, il rinvio è d’obbligo alla notissima sentenza della Corte di giustizia, grande sez., 6 ottobre 2015, in causa C-362/14, *Schrems*.

[10] “Clarifying Lawful Overseas Use of Data Act”, del 6 febbraio 2018 (H.R. 4943).

[11] “A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.” (18 U.S. Code § 2713. *Required preservation and disclosure of communications and records*).

Una posizione fortemente critica sulla compatibilità del *Cloud Act* rispetto ai principi in punto di tutela dei diritti fondamentali come interpretati dalla Corte di giustizia e dalla Corte EDU è stata espressa dal *Council of Bars and Law Societies of Europe* (CCBE), associazione che rappresenta oltre un milione di avvocati europei, nel documento *CCBE Assessment of the U.S. Cloud Act*

(disponibile ***on line***), ove si afferma: “The Cloud Act is in conflict with basic human rights, since it fails to provide the minimum standards set out by European Courts to restrict electronic surveillance by government. Both the European Court of Human Rights and the European Court of Justice have indicated a strong preference for prior judicial review and a requirement for a sufficient factual basis for any surveillance of an individual. Moreover, disclosure of personal data stored within the European Union to a US governmental agency based on a Cloud Act warrant violates the General Data Protection Regulation (GDPR). According to the GDPR provisions, a US warrant does not constitute a legal basis for such a transfer outside the European Union”.

[12]Ai sensi dell’art. 3, comma 4, dell’allegato 3 del decreto del Presidente del Consiglio di Stato “I difensori, le parti in proprio, i verificatori, i consulenti tecnici, i commissari ad acta e, in generale, tutti coloro che vengono ammessi a partecipare a un collegamento da remoto in videoconferenza utilizzano dispositivi dotati di videocamera e microfono, ed accedono al sistema di collegamento di cui all’articolo 2, comma 2, lettera b), [*Microsoft Teams*] unicamente tramite web browser, autenticandosi come ‘ospite/guest’ e immettono quale nome una stringa costituita obbligatoriamente dai seguenti dati nell’ordine indicato: «NUMERORG[spazio]ANNORG[spazio]INIZIALE COGNOME[spazio]INIZIALE NOME» del tipo «9999 2020 R. M. ». L’Avvocatura dello Stato utilizza un nome del tipo «AVVOCATURASTATO»”.

[13] Ai sensi dell’art. 2, comma 8, del decreto “all’atto del collegamento e prima di procedere alla discussione, i difensori delle parti o le parti che agiscono in proprio dichiarano, sotto la loro responsabilità, che quanto accade nel corso dell’udienza o della camera di consiglio non è visto né ascoltato da soggetti non ammessi ad assistere alla udienza o alla camera di consiglio, nonché si impegnano a non effettuare le registrazioni di cui al comma 11”. Il successivo comma 11 vieta la registrazione sia delle udienze, sia delle camere di consiglio svolte dai soli magistrati, nonché l’utilizzo di ogni strumento o funzione idoneo “a conservare nella memoria del sistema traccia delle dichiarazioni e delle opinioni espresse dai partecipanti all’udienza o alla camera di consiglio”.

[14] Art. 9 dell’allegato 3 al decreto.

[15] Si tratta, come è noto, del Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[16] Nel parere il riferimento all’art. 9, par. 2, lett. g) (relativo alle ipotesi in cui il trattamento di dati sensibili “è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell’Unione o degli Stati membri”) pare riconducibile ad un mero refuso, laddove è la lett. f) che ammette il trattamento anche di dati sensibili quando “è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali”. L’art. 10 del G.D.P.R., infine, ammette il trattamento dei dati personali relativi a condanne penali e reati soltanto sotto il controllo dell’autorità pubblica.

[17] Il riferimento è a Santi Romano, *Sui decreti-legge e lo stato di assedio in occasione del terremoto di Messina e Reggio Calabria,* in *Riv. dir. pubbl.,* 1909, I, 257.