Processo penale "a distanza" e diritto alla privacy: possibili profili di contrasto*

Pietro Insolera - Stella Romano

Abstract

L'articolo analizza le novità normative emergenziali introdotte dal d.l. 17 aprile 2020, n. 18, convertito nella legge n. 27 del 24 aprile 2020, come modificato dal d.l. 30 aprile 2020, n. 28, inerenti alla disciplina del c.d. processo penale a distanza. Ci si sofferma sui potenziali profili di frizione con il diritto alla privacy, che, com'è noto, gode di un robusto statuto di garanzia tanto a livello costituzionale interno, quanto a livello eurounitario e convenzionale. Si svolge in particolare una critica dell'individuazione, a mezzo provvedimento amministrativo del DGSIA del Ministero della Giustizia, degli applicativi Teams e Skype for Business, che determina l'applicabilità del *Cloud Act* statunitense, con importanti conseguenze negative per il trattamento dei dati giudiziari. Si conclude sottolineando l'insufficienza delle modifiche da ultimo apportate con il provvedimento del DGSIA del 21 maggio 2020 a garantire il rispetto dei fondamentali principi posti a presidio della privacy nel sistema interno e sovranazionale.

The article analyzes the new emergency regulations introduced by Decree Law no. 18 of 17 April 2020, converted into Law no. 27 of 24 April 2020, as modified by Decree Law no. 28 of 30 April 2020, relating to the regulation of the so-called remote criminal trial. Focus is given to the potential violations of the right to privacy, which enjoys strong protection both under domestic constitutional principles, as well as under CFREU and ECHR provisions. In particular, it is developed a critical assessment of the identification, by means of an administrative provision of the DGSIA of the Ministry of Justice, of the Teams and Skype for Business applications, which determines the applicability of the US Cloud Act, with important negative consequences for the treatment of judicial data. The article ends by highlighting the insufficiency of the changes recently adopted with the DGSIA provision of 21 May 2020 to comply with the fundamental principles of privacy protection in the internal and supranational legal systems.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a doppio cieco.

Sommario

Keywords

pandemia - processo penale da remoto – privacy – Carta di Nizza – CEDU

1. Premessa

Diversi contributi si sono già concentrati sui molteplici profili di incostituzionalità che paiono inficiare le disposizioni di matrice emergenziale sul cd. processo penale a distanza[1], relativi in particolare al *vulnus* del diritto di difesa, del giusto processo e del diritto di riservatezza[2] .

Obiettivo di questo breve articolo è riprendere e approfondire alcune di quelle considerazioni, soffermandosi specialmente sulle potenziali frizioni con il diritto di privacy,

[1] La disciplina è costituita dall'art. 83, c. 12, 12-*bis*, 12-*ter*, 12-*quater*, 12-*quater.1*, 12-*quater.2* e 12-*quinquies*, del d.l. 18/2020, convertito nella l. 27/2020, come modificato dal d.l. 28/2020. In particolare, il Governo con l'art. 2, c. 7 del d.l. 11/2020, reiterato con d.l. 18/2020, all'art. 83, c. 12, ha esteso le limitate ipotesi di collegamento da remoto previste dall'art. 146 bis disp. att. c.p.p., e sino al 31 maggio p.v., a qualsiasi udienza, per tutte le persone detenute, internate o in stato di custodia cautelare con modalità da individuarsi tramite provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Con provvedimento del 10 marzo 2020 il DGSIA ha dato sintetica attuazione alla delega, prescrivendo per le udienze penali l'utilizzo degli strumenti già adottati per i collegamenti di cui all'art. 146 bis disp. att. c.p.p. 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. In seguito, il Governo ha posto al Senato la questione di fiducia sul proprio maxiemendamento al disegno di legge di conversione del d.l. 18/2020 in data 9 aprile 2020 alla Camera ed in data 22 aprile 2020 al Senato. In tal modo, con la conversione nella l. 27/2020 sono stati inseriti, dopo il c. 12, ulteriori commi volti ad estendere il sistema dei collegamenti da remoto ben oltre le originarie previsioni di cui ai due decreti legge citati, ovvero alla generalità dei casi, "normalizzando temporaneamente", per così dire, il processo da remoto, che diviene il regime processuale ordinario a prescindere dallo stato di detenzione dell'imputato sino al 30 giugno 2020 (c. 12-*bis*). Il collegamento da remoto resta comunque "possibile" anche nella fase delle indagini preliminari (c. 12-*quater*) per il compimento di specifiche attività; nonché come modalità per le deliberazioni collegiali in camera di consiglio di tutti gli organi giurisdizionali, Corte di Assise compresa (c. 12-*quinquies*) e della Corte di Cassazione (c. 12-*ter* che richiama il c 12-*quinquies*). Infine, si è previsto con d.l. 28/2020 che il giudice, nei casi di cui sopra, debba comunque trovarsi nell'ufficio giudiziario e che il consenso delle parti al processo da remoto è necessario per le "udienze di discussione finale, in pubblica udienza o in camera di consiglio e a quelle nelle quali devono essere esaminati testimoni, parti, consulenti o periti" (art. 3, c. 1, lett. *c)* e lett. *d)*). Insiste, inoltre, un pericolo di normalizzazione del processo da remoto, in quanto con un emendamento all'art. 83 proposto dal Governo, si vuole introdurre la possibilità, previo accordo tra le parti, che i processi da remoto sia nel penale che nel civile possano tenersi fino al 31 dicembre 2021.

[2] Cfr. *Appunti sulle possibili eccezioni di illegittimità costituzionale in ordine alla disciplina del processo da remoto*, con il contributo degli avv.ti Federico Baffi, Gaia Caneschi, Federico Febbo, Francesco Fratini, Ettore Grenci, Pietro Insolera, Ladislao Massari e Stella Romano; coordinamento a cura di V. Manes - I. Pellizzone, consultabile in *camerepenali.it*; v. anche, per tutti questi profili, le analoghe considerazioni sviluppate da V. Manes - L. Petrillo - G. Sacconi, *Processo penale da remoto: prime riflessioni sulla violazione dei principi di legalità costituzionale e convenzionale*, in *dirittodidifesa.eu*, 6 maggio 2020.

che – come noto – gode di robusta protezione tanto nel sistema costituzionale interno, quanto in quello sovranazionale (eurounitario e convenzionale)[3].

A tale scopo, occorre in primo luogo ripercorrere sinteticamente il contenuto delle disposizioni rilevanti del d.l. 18/2020, convertito nella l. 27/2020.

La disposizione di cui al comma 12-*bis* dell'art. 83 permette il collegamento da remoto, da individuarsi e regolarsi con provvedimento del direttore generale dei sistemi informativi e automatizzati del Ministero della Giustizia (d'ora innanzi: DGSIA), per lo svolgimento delle udienze penali, con l'eccezione delle udienze di discussione finale o delle udienze istruttorie.

La disposizione di cui al comma 12-*quater* dell'art. 83 autorizza il giudice o il pubblico ministero in fase di indagini preliminari ad avvalersi del collegamento da remoto, da individuarsi e regolarsi con provvedimento del DGSIA, per il compimento di atti di indagini preliminari, 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.

Il DGSIA ha dato sintetica attuazione alla delega ed all'art. 3 si prescrive per le udienze penali l'utilizzo degli strumenti già adottati per i collegamenti di cui all'art. 146 *bis* disp. att. c.p.p. 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.

Tali disposizioni paiono porsi in contrasto con i principi costituzionali ed europei in materia di diritto alla riservatezza e di protezione dei dati personali, nella parte in cui introducono il collegamento da remoto per lo svolgimento delle udienze penali, rimettendone il vaglio all'autorità procedente da remoto laddove, con riferimento alla fase delle indagini preliminari, l'individuazione dell'opportunità del collegamento da remoto viene affidata alla valutazione dell'autorità giudiziaria al ricorrere dell'unica ed esclusiva condizione che la presenza fisica non possa essere assicurata per le esigenze di contenimento della diffusione del virus COVID – 19, senza che entrambe le disposizioni contengano alcuna precisa e chiara specificazione in merito al trattamento dei dati personali, oggetto della trasmissione attraverso il collegamento virtuale.

Ciò appare di maggior rilievo, laddove i dati oggetto di trattamento dal sistema informatico utilizzato nel collegamento da remoto appartengono al possibile *status* di "indagato" o "imputato" nel procedimento penale (cd. dati giudiziari). D'altronde, il d.lgs. 51/ 2018[4] – completamente ignorato dal legislatore dell'emergenza – ha disposto la piena applicabilità della disciplina di protezione dati, anche ai trattamenti di dati svolti nell'esercizio della funzione giurisdizionale.

Con riguardo al costituzionalmente problematico utilizzo di provvedimenti amministrativi del DGSIA, occorre preliminarmente richiamare i profili di criticità sollevati

[3] Cfr. *Appunti sulle possibili eccezioni di illegittimità costituzionale*, cit., 6-10.

[4] Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (18G00080).

dai 21 quesiti di cui alla nota dell'Unione Camere Penali Italiane indirizzata al Garante per la protezione dei dati personali in data 14 aprile 2020[5], relativi ai plurimi punti di frizione dell'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 con il d.lgs. 51/2018, in particolare laddove individuano i programmi commerciali *Skype for Business* e *Teams*, della società statunitense Microsoft Corporation, quali piattaforme per lo svolgimento del processo penale da remoto.

Come rilevato nella successiva lettera del Presidente del Garante per la protezione dei dati personali al Ministro della Giustizia il 16 aprile 2020[6], il trattamento dei dati personali pone seri problemi di compatibilità con la disciplina *ex* d.lgs. 51/2018, stante l'applicabilità del *Cloud Act* statunitense[7], che attribuisce alle autorità americane di contrasto un ampio potere acquisitivo di dati e informazioni.

Il Garante ha poi condiviso le ulteriori perplessità espresse dall'UCPI in merito alla «tipologia di dati eventualmente memorizzati da Microsoft Corporation per finalità proprie, del servizio o commerciali; sui soggetti legittimati all'accesso ai metadati delle sessioni e, in particolare, sull'eventualità che Microsoft Corporation o un amministratore di sistema possa desumere, dai metadati nella sua disponibilità, alcuni dati "giudiziari" particolarmente delicati quali, ad esempio, la condizione di soggetto sottoposto alle indagini o di imputato, magari *in vinculis*».

Il Garante ha osservato altresì che si tratta di temi sicuramente rilevantissimi e degni, pur nella condizione emergenziale che stiamo vivendo, della massima attenzione, al fine di coniugare esigenze di giustizia, tutela della salute e protezione dati.

Infine, il Garante ha rilevato criticamente che il Governo ha omesso di consultarsi preventivamente con la Sua Autorità, «passaggio tutt'altro che formale» per stabilire le adeguate opzioni di disciplina, tramite ragionevole contemperamento dei diversi interessi in gioco, in un settore così delicato.

2. Il processo "a distanza" al vaglio del diritto costituzionale alla riservatezza

Le disposizioni di cui all'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 hanno l'obiettivo di consentire la prosecuzione dell'attività giudiziaria penale, volta ad accertare fatti di reato e responsabilità individuali per punire i responsabili secondo la legge e proteggere la sicurezza pubblica, garantendo al contempo adeguatamente, nel contesto di un'eccezionale crisi sanitaria causata dalla pandemia da Covid 19, la salute individuale degli operatori del diritto e la salute collettiva.

Appurato che si tratta di scopi legittimi, occorre verificare se il sacrificio dei diritti individuali – e, segnatamente, per quel che rileva, il diritto alla privacy, in specifica

[5] *Processo penale da remoto e protezione dei dati personali. L'Unione scrive al Garante*, 14 aprile 2021, consultabile in *camerepenali.it*.

[6] Processo penale da remoto: lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro della Giustizia, Alfonso Bonafede, 17 aprile 2021, doc. web n. 9316889, consultabile in *garanteprivacy.it*.

[7] The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943)

relazione alla raccolta, alla conservazione e al trattamento di alcuni dati "giudiziari" particolarmente delicati quali, ad esempio, la condizione di soggetto sottoposto alle indagini o di imputato, magari *in vinculis*, implicato dallo strumento normativo utilizzato – possa dirsi necessario e dunque proporzionato agli obiettivi, stante l'indisponibilità di misure meno invasive, ma egualmente adeguate allo scopo.

Con specifico riguardo all'individuazione del parametro costituzionale, si tratta del diritto alla riservatezza dell'individuo, che svolge la propria personalità anche in quel luogo virtuale rappresentato dal sistema informatico.

In tale prospettiva, la portata della "riservatezza informatica", da un lato, appare più estesa della dimensione originaria della privacy, e, da un altro lato, è espressione del riconoscimento dei diritti dell'individuo in quanto partecipe della comunità virtuale[8].

Sul piano del fondamento costituzionale, il diritto alla riservatezza dei dati personali è manifestazione del diritto fondamentale all'intangibilità della sfera privata (Corte cost., 23 luglio 1991, n. 366), che attiene alla tutela della vita degli individui nei suoi molteplici aspetti. Un diritto che trova riferimenti nella Costituzione italiana, già riconosciuto, in relazione a molteplici ambiti di disciplina, nella giurisprudenza della Corte costituzionale (Corte cost., 21 febbraio 2019, n. 20; 11 giugno 2009, n. 173; 14 novembre 2006, n. 372; 24 aprile 2002, n. 135; 11 marzo 1993, n. 81; 23 luglio 1991, n. 366;26 giugno 1969, n. 104; 26 giugno 1970, n. 112; 6 aprile 1973, n. 34; 12 aprile 1973, n. 38; 5 febbraio 1975, n. 20)[9].

Dato costante nella giurisprudenza costituzionale sopra richiamata è, inoltre, l'esigenza che la riservatezza, in tutte le sue specifiche declinazioni e variegati contenuti di protezione, sia oggetto di un ragionevole bilanciamento complessivo in sede legislativa con gli altri valori e interessi rilevanti (v. spec. Corte cost., 24 febbraio 1994, n. 63; 14 novembre 2006, n. 372, *mutatis mutandis* v. soprattutto la nota Corte cost., 9 maggio 2013, n. 85[10]), ed in particolare con l'istanza di repressione dei fenomeni criminosi.

Invero, se con riferimento alla conservazione tradizionale dei dati giudiziari, la Corte costituzionale nella sentenza n. 173/2009*,* qualificando come fondamentale il diritto

[8] V. De Rosa, *La formazione di regole giuridiche per il* cyberspazio, in *Il diritto dell'informazione e dell'informatica*, 2003, 2, 377.

[9] Cfr. l'ampia disamina dell'evoluzione giurisprudenziale e dottrinaria di M. Luciani, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, in *astrid-online.it* , 4 ottobre 2018.

[10] «Tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre «sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro» (sentenza n. 264/2012). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona. […] «La Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi. La qualificazione come "primari" dei valori dell'ambiente e della salute significa pertanto che gli stessi non possono essere sacrificati ad altri interessi, ancorché costituzionalmente tutelati, non già che gli stessi siano posti alla sommità di un ordine gerarchico assoluto. Il punto di equilibrio, proprio perché dinamico e non prefissato in anticipo, deve essere valutato – dal legislatore nella statuizione delle norme e dal giudice delle leggi in sede di controllo – secondo criteri di proporzionalità e di ragionevolezza, tali da non consentire un sacrificio del loro nucleo essenziale». Cfr. in dottrina: M. Cartabia, *Ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, in A. Giorgis - E. Grosso – J. Luther, *Il costituzionalista riluttante. Scritti per Gustavo Zagrebelsky*, Torino, 2016, 463 ss.

alla riservatezza e riconoscendogli altresì pari dignità di tutela rispetto al diritto inviolabile alla riservatezza della corrispondenza, aveva affermato che «non è garantita, nelle condizioni normative ed organizzative attuali, una adeguata tenuta della segretezza degli atti custoditi negli uffici giudiziari, come purtroppo dimostrano le frequenti 'fughe' di notizie e documenti», la presente normativa presenta un importante *vulnus* nella misura in cui non specifica precise modalità atte a garantire la riservatezza e l'integrità dei sistemi di collegamento da remoto e rinviando alla fonte amministrativa per la loro concreta operatività.
Il legislatore, nelle disposizioni censurate, ha infatti fatto prevalere irragionevolmente le esigenze di tutela della salute e di repressione dei reati a discapito della riservatezza degli indagati/imputati.
Ciò è manifestato plasticamente dal fatto che si sia delegato a una fonte amministrativa, il provvedimento della DGSIA, il compito di "individuare e regolamentare i collegamenti" necessari a consentire lo svolgimento delle udienze da remoto in modo da «garantire il contraddittorio e l'effettiva partecipazione delle parti» (12-*bis*), o, in fase di indagini preliminari, affidandone la valutazione all'autorità procedente nei casi in cui la presenza fisica «non può essere assicurata senza mettere a rischio le esigenze di contenimento della diffusione del virus COVID-19» (12-*quater*), omettendosi ogni previo confronto con il Garante per la protezione dei dati personali, in una materia di sua esclusiva competenza.
Emergono dunque dall'*iter legis* una insufficiente ponderazione degli interessi in gioco e una mancata valutazione – anche attraverso indagini empiriche, approfondimenti tecnici, valutazioni di impatto – di strumenti alternativi meno invasivi per i diritti individuali ma comunque idonei a perseguire lo scopo, tali da risolversi in un eccessivo sacrificio dei diritti di riservatezza.

3. (*segue*) Spunti di diritto eurounitario sulla protezione dei dati personali

Il diritto alla protezione dei dati personali è attratto al livello dell'ordinamento dell'Ue, dove non solo riceve un articolato riconoscimento nel catalogo dei diritti fondamentali (art. 8 Carta di Nizza) e nelle fonti di diritto primario (art. 16 TFUE), ma trova anche compiuta disciplina mediante una fonte secondaria idonea a realizzare il livello massimo di armonizzazione della legislazione degli Stati membri, di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.
Peraltro, proprio in materia di diritto alla protezione dei dati personali, la Corte costituzionale con sentenza n. 20/2019 ha stabilito che «i principi e i diritti enunciati nella CDFUE intersecano in larga misura i principi e i diritti garantiti dalla Costituzione italiana (e dalle altre Costituzioni nazionali degli Stati membri), e che la prima costituisce pertanto 'parte del diritto dell'Unione dotata di caratteri peculiari in ragione del suo contenuto di impronta tipicamente costituzionale'», derivandone che «va preservata l'opportunità di un intervento con effetti erga omnes di questa Corte, in virtù del principio che situa il sindacato accentrato di legittimità costituzionale a fondamento

dell'architettura costituzionale (art. 134 Cost.), precisando che, in tali fattispecie, la Corte costituzionale giudicherà alla luce dei parametri costituzionali interni, ed eventualmente anche di quelli europei (*ex* artt. 11 e 117, primo comma, Cost.), comunque secondo l'ordine che di volta in volta risulti maggiormente appropriato».

I principi che devono governare il trattamento sono sanciti nell'art. 5, c. 1, del citato regolamento e, tra di essi, assumono particolare rilievo quelli che consistono: nella limitazione della finalità del trattamento (lettera b) e nella "minimizzazione dei dati", che si traduce nella necessità di acquisizione di dati adeguati, pertinenti e limitati a quanto strettamente necessario alla finalità del trattamento (lettera c).

Ancora, un riferimento al necessario bilanciamento tra diritti si trova nelle premesse al regolamento 2016/679/UE (considerando 4), ove si legge che «[i]l diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». Tale corollario normativo non rappresenta altro che il precipitato dell'art. 52, par. 1, della Carta di Nizza, che riconosce, pertanto, che possono essere apportate limitazioni all'esercizio di diritti come quelli sanciti dagli artt. 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà, nel rispetto del principio di proporzionalità.

In definitiva, la disciplina europea, pur riconoscendo un ampio margine di regolazione autonoma e di dettaglio agli Stati membri con riguardo a certe tipologie di trattamento (in specie con riferimento alla tutela della salute pubblica: art. 32 Cost. ed art. 35 della Carta di Nizza), impone loro il principio di proporzionalità del trattamento che, rappresenta il fulcro della giurisprudenza della Corte di giustizia dell'Unione europea in materia[11].

In particolare, occorre rimarcare le criticità poste dalla normativa applicabile alle piattaforme individuate, su delega dell'art. 83, d.l. 18/2020, con provvedimenti amministrativi della DSGIA, *Microsoft Teams* e *Skype for Business*, il *Cloud Act*, che consente alle autorità statunitensi, forze dell'ordine e agenzie di *intelligence*, di acquisire dati informatici dagli operatori di servizi di *cloud computing* «*regardless of whether such communications, record or other informations is located within or outside of USA*», ossia indipendentemente dal fatto che tali comunicazioni, registrazioni o altre informazioni si trovino all'interno o all'esterno degli Stati Uniti.

Gli *Internet Service Provider*, interessati dalla misura, sono le compagnie private sottoposte alla giurisdizione degli Stati Uniti ovvero le società costituite negli Stati Uniti e le loro filiali all'estero (per quel che qui rileva, la Microsoft Corporation), ma anche le società europee che hanno una filiale negli Stati Uniti o che operano nel mercato americano. Per quanto riguarda i dati richiesti e la natura della misura, quest'ultima è considerata una misura nazionale e le autorità statunitensi devono rispettare rigorosamente le tutele legislative e costituzionali proprie degli Stati Uniti: a seconda dei casi mandato, ordinanza o ordine di esibizione amministrativo[12].

---

[11] CGUE, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e altri* (2003) e cause riunite C-92/09 e 93/09, *Volker und Markus Schecke e Eifert* (2010).

[12] Cfr. B. Calderini, *Cloud act, la norma USA che fa a pugni con la privacy europea: i nodi*, all'URL, in

La disciplina statunitense relativa al trattamento dei dati personali applicabile alle piattaforme individuate dal DGSIA *Microsoft Teams* e *Skype for Business* è stata criticata in questi termini dal Consiglio degli Ordini Forensi d'Europa: «La legge CLOUD è in conflitto con i diritti umani fondamentali, poiché non fornisce gli standard minimi stabiliti dalle corti europee per limitare la sorveglianza elettronica da parte del governo. Secondo la giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia europea, qualsiasi interferenza con il diritto alla privacy deve essere conforme alla legge, per uno scopo legittimo e limitato a ciò che è necessario in una società democratica»[13].

Si porrebbero, dunque, profili rilevanti di limitazione del nucleo essenziale del diritto alla riservatezza, con riferimento al trattamento dei dati giudiziari all'interno di circuiti, posti al di fuori dal controllo di soggetti terzi ed indipendenti, come, invece, richiesto dalla normativa derivata europea[14], passibili altresì di accessi occulti ed in maniera generalizzata, oltre il limite della stretta necessità, pregiudicando l'integrità e la sicurezza dei dati stessi.

In conclusione, può affermarsi che, alla luce di questi principi, le disposizioni di cui all'art. 83, c. 12-*bis* e 12-*quater,* laddove individuano tramite delega alla DSGIA gli applicativi della Microsoft Corporations *Microsoft Teams* e *Skype for Business*, assoggettati all'applicazione del *Cloud Act*, espongono ad un pericolo di lesione eccessivo i cd. dati giudiziari di indagati ed imputati, senza rispettare – come visto sopra – gli standard di protezione minima garantiti dalle disposizioni interne ed europee.

L'ampio potere di acquisizione, archiviazione, trattamento delle autorità governative statunitensi può comportare peraltro – osserviamo infine – ulteriori pregiudizi. Si pensi, ad esempio, al soggetto sottoposto a procedimento penale celebrato da remoto, conclusosi con pronuncia di proscioglimento, che si veda poi rigettata la domanda per ottenere il visto di lavoro o di studio negli USA, a causa di dati giudiziari illegittimamente acquisiti e magari conservati oltre un certo limite temporale, in violazione del diritto all'oblio[15].

Parimenti dubbia la compatibilità con l'art. 48 del Regolamento Generale sulla Protezione dei Dati (regolamento (UE) 2016/679) sul trasferimento di dati personali verso

agendadigitale.eu, 11 giugno 2019. La normativa, emanata per semplificare le attività di indagine penali transfrontaliere superando il precedente sistema MLAT, è stata sottoposta a numerose critiche anche negli USA: cfr. ad es. N.S. Giuliani, *The Cloud Act is a Dangerous Piece of Legislation*, in *aclu.org*, 13 marzo 2018; in dottrina, v. ad es. S. Biligic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the Cloud Act*, in *Harvard Journal of Law & Technology*, 32(1), 2018, 321 ss., spec. 347 ss.

[13] Cfr. *CCBE Assessment of the U.S. Cloud Act,* 28 febbraio 2019, consultabile in *ccbe.eu*. Per una valutazione meno critica, cfr. O. Pollicino - M. Bassini, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.eu*, 26 ottobre 2018, spec. § 2.

[14] L'art. 10 del GDPR prevede che «il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica».

[15] In tale situazione, potrebbero prospettarsi ulteriori profili di contrasto con l'art. 117, c. 1, Cost., in relazione agli artt. 14 e 2, Prot. n. 4, CEDU.

Paesi terzi[16].

A tale riguardo, viene in rilievo quanto statuito dalla Corte di giustizia dell'Unione europea nella causa *Schrems* del 6 ottobre 2015[17] che riguardava la tutela delle persone fisiche con riguardo al trasferimento dei loro dati personali verso paesi terzi, nella fattispecie, gli Stati Uniti.

I trasferimenti di dati verso gli Stati Uniti si basavano su una decisione di adeguatezza adottata dalla Commissione nel 2000, che all'epoca consentiva trasferimenti verso le società statunitensi che autocertificavano la protezione da parte loro dei dati personali trasferiti dall'UE e il rispetto dei cosiddetti "principi di approdo sicuro" (c.d. *Safe Harbour*). Quando la causa è stata portata dinanzi alla CGUE, quest'ultima ha esaminato la validità della decisione della Commissione alla luce della Carta ricordando che la protezione dei diritti fondamentali nell'UE richiede che le deroghe e le restrizioni a tali diritti operino solo entro i limiti dello stretto necessario. La CGUE ha ritenuto che una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche «pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta».

Il diritto sarebbe svuotato di significato qualora i pubblici poteri statunitensi fossero autorizzati ad accedere alle comunicazioni su base casuale, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente individuati.

Da ultimo occorre sinteticamente rilevare che, sebbene la nuova Decisione della Commissione europea di adeguatezza riguardo al trasferimento dei dati dall'UE agli U.S.A. del 12 luglio 2016, c.d. *Privacy Shield*[18], abbia in parte sanato alcune delle gravi carenze censurate dalla Corte di giustizia nella sentenza *Schrems*, allo stato permangono diversi profili di dubbia compatibilità, in relazione al potere ancora molto invasivo delle autorità statunitensi, difficilmente in grado di assicurare un livello di protezione dei dati adeguato e sostanzialmente equivalente a quello predisposto dal sistema normativo dell'UE[19].

---

[16] Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

[17] CGUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC] (2015).

[18] Cfr. la scheda "Privacy Shield" del Garante privacy, 26 luglio 2016, doc. web n. 5306161, al sito *garanteprivacy.it*

[19] Per considerazioni più diffuse sul punto, cfr. senza pretesa di completezza: S. Crespi, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016, 687 ss., spec. 710 ss.; R. Ferraro, *Lo EU-U.S.* Privacy Shield. *Una risposta insufficiente alle richieste della Corte di giustizia dell'Unione europea nella sentenza* Safe Harbour*?*, in *Diritto del commercio internazionale*, 3, 2017, 635 ss.

4. Il processo "a distanza" nel *focus* del diritto convenzionale

Il diritto alla riservatezza trova tutela nell'art. 8 della Convenzione europea dei diritti dell'uomo che dispone: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».
Ai sensi del paragrafo 2 le ingerenze dell'autorità sono legittime in presenza di tre requisiti: 1) una previsione legislativa, rispetto alla quale la giurisprudenza europea accentua il riferimento all'accessibilità e alla conoscibilità delle fonti normative e della giurisprudenza, essendo necessario che il cittadino possa ragionevolmente prevedere le conseguenze delle proprie azioni; 2) il perseguimento di una delle finalità legittime previste tassativamente dalla norma con riferimento sia a molteplici interessi dello Stato e della collettività, sia alla tutela dei diritti e delle libertà altrui; 3) la necessità della misura in una società democratica per il conseguimento degli obiettivi sopra indicati. In questa ultima prospettiva della "necessità" si inserisce il criterio della proporzionalità tra ingerenza e finalità legittima perseguita.
Le considerazioni dianzi svolte consentono di apprezzare un primo profilo di possibile contrasto dell'art. 83, c. 12-*bis* e 12-*quater*, cit. con l'art. 117, c. 1, Cost., in relazione all'art. 8 CEDU. L'art. 8, par. 2, Convenzione EDU, dispone che non può esservi ingerenza di una autorità pubblica nell'esercizio del diritto alla vita privata a meno che tale ingerenza sia prevista dalla legge.
La Corte di Strasburgo[20] ha statuito che tale previsione non si limita a richiedere la conformità con la normativa nazionale – più che dubbia, come si è visto, nel caso di specie – ma riguarda anche la qualità della legge, richiedendo che sia compatibile con la *rule of law*. Si è così affermato che la disposizione nazionale deve essere chiara, prevedibile e adeguatamente accessibile[21]. Essa dev'essere sufficientemente prevedibile, così da mettere nelle condizioni gli individui di agire in conformità alla legge[22], e deve tracciare chiaramente i confini della portata della discrezionalità di cui godono le pubbliche autorità. Per esempio, come la Corte ha illustrato nel contesto della sorveglianza, la legge deve essere sufficientemente chiara nella sua formulazione testuale da fornire ai cittadini una indicazione adeguata circa le condizioni e circostanze in cui le autorità hanno il potere di ricorrere a qualsivoglia misura di sorveglianza segreta e

[20] I riferimenti del *case law* convenzionale d'ora innanzi citati sono traduzioni di passaggi tratti dai *Reports: Guide on Article 8 of the European Convention on Human Rights* e *Factsheet – Personal data protection*, entrambi disponibili all'URL *echr.coe.int*.

[21] CEDU, *Amann c. Svizzera* [GC], ric. 27798/95 (2000), § 56; cfr. anche *Malone c. Regno Unito*, ric. 8691/79 (1984), § 66; *Silver e a. c. Regno Unito*, ricc. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75(1983), § 88).

[22] CEDU, *Amann c. Svizzera,* cit., § 50; cfr. anche *Kopp c. Svizzera*, ric. 23224/94 (1998).

raccolta di dati personali[23]. Si è altresì statuito che il requisito della chiarezza si applica alla portata della discrezionalità esercitata dalle pubbliche autorità. La norma nazionale deve indicare con ragionevole chiarezza la portata e il modo dell'esercizio della discrezionalità rilevante conferita alle pubbliche autorità, in modo tale da assicurare agli individui un grado minimo di protezione al quale loro hanno il diritto in forza della *rule of law* in una società democratica[24].

Per quanto attiene al diritto alla protezione dei dati, nella causa *Rotaru c. Romania*, la Corte EDU ha rilevato che la legge nazionale autorizzava la raccolta, la registrazione e l'archiviazione in fascicoli segreti di informazioni rilevanti per la sicurezza nazionale, ma non stabiliva limiti all'esercizio di tali poteri, che rimanevano *a discrezione delle autorità*. Il diritto nazionale non definiva, per esempio, il tipo d'informazioni che avrebbero potuto essere trattate, le categorie di persone nei cui confronti si sarebbero potute adottare misure di sorveglianza, le circostanze in cui tali misure si sarebbero potute prendere o la procedura da seguire. La Corte di Strasburgo ha pertanto concluso che il diritto nazionale non rispettava il requisito di prevedibilità ai sensi dell'art. 8 della CEDU[25].

Ancora, la causa *Vukota-Bojić c. Svizzera* riguardava la sorveglianza segreta di una richiedente un'assicurazione sociale, da parte di *investigatori privati commissionati* dalla sua compagnia di assicurazione. La Corte EDU ha ritenuto che, sebbene la misura di sorveglianza oggetto del ricorso fosse stata ordinata da una compagnia di assicurazione privata, a tale società era stato riconosciuto dallo Stato il diritto di erogare prestazioni rientranti nell'assicurazione medica obbligatoria e di riscuotere premi assicurativi. I giudici di Strasburgo hanno, in particolar modo, statuito che uno Stato non può esonerare sé stesso dalle responsabilità previste dalla Convenzione, delegando i propri obblighi a enti privati o persone fisiche. Affinché l'ingerenza potesse essere "conforme alla legge", il diritto nazionale avrebbe dovuto fornire garanzie sufficienti contro l'abuso per ingerenza nei diritti di cui all'articolo 8 della CEDU. Nel caso in esame, la Corte EDU ha concluso che vi era stata violazione dell'articolo 8 della CEDU, in quanto il diritto nazionale non aveva indicato con sufficiente chiarezza la portata e le modalità dell'esercizio del potere discrezionale di esercitare una sorveglianza segreta su una persona assicurata, accordato a compagnie di assicurazione che agiscono in qualità di autorità pubbliche nelle controversie in materia[26].

Ebbene, se il requisito di *lawfulness* è ricostruito in termini così stringenti nella giurisprudenza convenzionale, che richiede vi siano salvaguardie idonee ad assicurare i diritti individuali protetti dall'art. 8, non può che escludersi che la norma censurata sia in grado di soddisfare tale standard di garanzia.

Come si è già detto, infatti, il contrasto con il principio di legalità processuale è aggra-

[23] CEDU, *Shimovolos c. Russia*, ric. 30194/09 (2011), § 68.

[24] CEDU, *Piechowicz c. Polonia,* ric. 20071/07 (2012), § 212.

[25] CEDU, *Rotaru c. Romania* [GC], ric. 28341/95 (2000), § 57; cfr. anche *Association for European Integration and Human Rights e Ekimdzhiev c. Bulgaria*, ric. 62540/00 (2007); *Shimovolos c. Russia*, ric. 30194/09 (2011); e *Vetter c. Francia*, ric. 59842/00 (2005).

[26] CEDU, *Taylor-Sabori c. Regno Unito*, ric. 47114/99 (2002) § 48; *Vukota-Bojić c. Svizzera*, ric. 61838/10 (2016), § 77.

vato dall'ampiezza del margine di intervento concesso al menzionato provvedimento del DSGIA, per la disciplina dei collegamenti da remoto; consegnando parallelamente al giudice un compito altrettanto generico ed indeterminato, ossia quello di assicurare che lo svolgimento dell'udienza avvenga «con modalità idonee a salvaguardare il contraddittorio e l'effettiva partecipazione delle parti»: così rimettendo alla discrezionale ed insindacabile valutazione del giudice (il gravoso onere di garantire) aspetti essenziali e fondamentali delle garanzie previste dagli artt. 24 e 111 Cost., con una latitudine valutativa difficilmente compatibile con quando la stessa Corte costituzionale ha stabilito ripudiando apertamente – nell'ordinanza n. 24/2017 – l'idea del "giudice di scopo", ritenuta incompatibile con la stessa soggezione del giudice alla legge (art. 101, c. 2, Cost.).

Siffatto *vulnus* al principio di legalità, sotto il profilo dell'eccesso di discrezionalità, tale da sfociare in arbitrio, compromette anche il requisito di *lawfulness* della misura che interferisce sul diritto alla riservatezza, per quanto concerne il trattamento dei dati personali, affidato, attraverso un provvedimento amministrativo, a una società commerciale di diritto statunitense assoggettata all'applicabilità di una normativa, il *Cloud Act* statunitense, sulla cui effettiva idoneità a preservare la riservatezza dei dati giudiziari è ragionevole nutrire più di un dubbio.

Se si ritenesse l'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 conforme al requisito di *lawfulness*, occorrerebbe comunque verificarne la legittimità costituzionale rispetto all'art. 117, c. 1, Cost. in rapporto all'art. 8, c. 2, CEDU, ove impone che la misura che interferisce sul diritto alla vita privata, in una società democratica, sia necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Sotto questo profilo, non vi è dubbio che gli scopi perseguiti dalla disposizione censurata, che intende consentire la prosecuzione dell'attività giudiziaria penale in condizioni di sicurezza durante una grave emergenza sanitaria pandemica (e dunque: pubblica sicurezza, difesa dell'ordine e prevenzione dei reati, protezione della salute, protezione dei diritti e delle libertà altrui, tutti da ritenersi "*pressing social needs*"), siano legittimi.

Occorre però valutare se la misura adottata risulti proporzionata rispetto ai suddetti scopi.

In particolare, è necessario stabilire se il significativo sacrificio dei cd. dati giudiziari determinato dall'individuazione delle piattaforme *Microsoft Teams* e *Skype for Business* con provvedimento amministrativo da parte della DSGIA e dalla conseguente applicabilità del *Cloud Act* è necessario, ovvero se, al contrario, era possibile perseguire l'obiettivo di assicurare la prosecuzione dell'attività giudiziaria penale in condizioni di sicurezza durante una grave emergenza sanitaria pandemica con la stessa efficacia attraverso strumenti meno afflittivi per il diritto di riservatezza, sotto il peculiare profilo della conservazione e del trattamento dei dati giudiziari dell'indagato/imputato.

A tale proposito, le stesse caratteristiche della procedura legislativa d'urgenza e l'omessa consultazione del Garante per la protezione dei dati personali indicano come non siano state valutate con sufficiente ponderazione/attenzione modalità alternative più adeguate a salvaguardare i dati giudiziari, inevitabilmente disvelati nell'ambito dell'at-

tività processuale penale.

Una più approfondita analisi tecnica, empirica e di impatto, pur nei limiti delle possibilità concesse da un assai complicato contesto emergenziale, avrebbe permesso al legislatore di selezionare più ragionevolmente piattaforme per lo svolgimento delle udienze penali meno rischiose per la privacy[27].

Insomma, l'*iter legis* conferma un inadeguato e irrazionale bilanciamento tra i valori in gioco, a tutto detrimento della protezione dei cd. dati giudiziari, tale da produrre una misura che interferisce sul piano sostanziale eccessivamente nel diritto alla vita privata.

D'altra parte, nel *case law* della Corte EDU emerge che, per determinare la proporzionalità generale di una misura, la Corte valuta in primo luogo le scelte legislative che ne stanno alla base. La qualità del controllo parlamentare sulla effettiva necessità della misura è di particolare importanza sotto questo profilo[28].

Ed invero, la Corte europea, proprio nel settore di nostro interesse, inerente al c.d. "*storage and use of personal data*" nell'amministrazione della giustizia penale, è intervenuta a più riprese accertando la violazione dell'art. 8 da parte di misure statuali viziate da sproporzione rispetto a scopi legittimi.

Nella sentenza *S. and Marper c. Regno Unito*[29], la Corte afferma in termini generali che «La protezione dei dati personali è di fondamentale importanza affinché la persona possa godere del suo diritto al rispetto della vita privata e familiare, garantito dall'articolo 8. Il diritto nazionale deve accordare salvaguardie appropriate per impedire qualsivoglia uso dei dati personali che possa essere incoerente con le garanzie di questo articolo […] la necessità di tali garanzie è ancora più forte laddove è in gioco la protezione di dati personali sottoposti a procedure di trattamento automatico, non ultimo quando tali dati sono utilizzati per scopi di polizia. La normativa interna dovrebbe specialmente assicurare che tali dati siano rilevanti e non eccessivi in rapporto agli scopi per cui sono archiviati; e conservati in una forma che permetta l'identificazione dei titolari dei dati non oltre il tempo necessario rispetto allo scopo per il quale i dati sono archiviati [...] Essa deve accordare anche adeguate garanzie sul fatto che i dati conservati sono stati efficacemente protetti da un utilizzo erroneo e dall'abuso»[30].

---

[27] Si sarebbe potuto trarre spunto, ad esempio, dall'esperienza del cd. Processo Civile Telematico, oppure collocare i collegamenti da remoto per lo svolgimento delle udienze penali nella Rete Unica Giustizia (c.d. R.U.G.), e non nella rete internet pubblica, ove i dati giudiziari sono ben più facilmente intercettabili; ovvero, infine, si sarebbero potute scegliere altre piattaforme gestite da *software* italiani, come *iorestoacasa.work*, consorzio che fornisce attualmente la dorsale internet al CNR e alle Università italiane, in grado di garantire standard di protezione ben più elevati. Cfr. ad es. P. Dimalio, *I processi targati Microsoft: arriva la spia in tribunale?*, in *Il Fatto Quotidiano*, 27 aprile 2020.

[28] Cfr. CEDU, *Animal Defenders International c. Regno Unito* [GC], ric. 48876/08 (2013) § 108.

[29] CEDU, ric. 30562/04 (2008), § 103.

[30] Il caso *S. and Marper* riguardava la conservazione a tempo indefinito in un archivio delle impronte digitali, dei campioni cellulari e dei profili di DNA dei ricorrenti dopo che un procedimento penale nei loro confronti era terminato con una assoluzione in un caso e sospeso nell'altro. La Corte ha accertato una violazione dell'art. 8, ritenendo che la conservazione in questione aveva integrato un'interferenza sproporzionata nell'esercizio del diritto dei ricorrenti al rispetto della vita privata e non poteva essere considerata necessaria in una società democratica. La Corte ha ritenuto in particolare che l'utilizzo di moderne tecniche scientifiche nel sistema di giustizia penale non poteva essere consentito ad ogni costo e senza bilanciare accuratamente i potenziali benefici dell'uso estensivo di tali tecniche a fronte di importanti interessi riconducibili alla riservatezza. Ogni Stato Contraente che rivendica un ruolo

Nel caso *M.M. c. Regno Unito* del 13 novembre 2012[31], la Corte ha dichiarato che vi era stata una violazione dell'articolo 8 della Convenzione, in quanto non erano state approntate sufficienti garanzie nel sistema per la conservazione e la rivelazione dei dati del casellario giudiziario al fine di garantire che i dati relativi alla vita privata del richiedente non fossero divulgati in violazione del suo diritto al rispetto della vita privata. La Corte ha osservato in particolare che, sebbene i dati contenuti nel casellario giudiziale fossero, in un certo senso, informazioni pubbliche, la loro sistematica memorizzazione nei registri centrali significava che erano disponibili per la rivelazione molto tempo dopo l'evento quando probabilmente tutti gli altri, tranne la persona interessata, se ne sarebbero dimenticati, specialmente laddove, come nel caso del richiedente, l'ammonimento si era verificata in privato.

Nel caso *Brunet c. Francia* del 18 settembre 2014[32]**,** il ricorrente si è lamentato in particolare di un'interferenza con la sua vita privata a seguito dell'aggiunta al database di polizia STIC (sistema per l'elaborazione dei reati registrati) - contenente informazioni da rapporti di indagine, elencando le persone coinvolte e le vittime - dopo l'interruzione del procedimento penale a suo carico. La Corte ha ritenuto che vi fosse stata una violazione dell'articolo 8 della Convenzione, rilevando che lo Stato francese aveva oltrepassato il suo potere discrezionale di decidere ("margine di apprezzamento") su tali questioni: la conservazione poteva essere considerata una violazione sproporzionata del diritto della ricorrente al rispetto della sua vita privata. La Corte ha ritenuto in particolare che il ricorrente non avesse avuto una reale possibilità di chiedere la cancellazione dalla banca dati delle informazioni che lo riguardavano e che la durata della conservazione di tali dati, 20 anni, potesse essere assimilata, se non alla conservazione a tempo indefinito, a quanto avveniva di regola piuttosto che a un limite massimo.

Infine, nel caso *Gaughran c. Regno Unito* del 13 febbraio 2020[33], riguardante una denuncia della conservazione indefinita di dati personali (profilo del DNA, impronte digitali e fotografie), la Corte ha ritenuto che vi fosse stata una violazione dell'articolo 8 della Convenzione, constatando che il Regno Unito aveva superato il margine di apprezzamento accettabile e che la conservazione in questione costituiva un'interferenza sproporzionata con il diritto del richiedente al rispetto della vita privata, che non poteva essere considerato necessario in una società democratica.

---

di pioniere nello sviluppo di nuove tecnologie ha una speciale responsabilità di "trovare il giusto compromesso". La Corte ha concluso che la natura totale e indiscriminata dei poteri di conservazione delle impronte digitali, dei campioni cellulari e dei profili di DNA di persone sospettate ma non condannate per i reati, così come applicata nel caso di specie, non era riuscita a bilanciare adeguatamente gli interessi pubblici e privati contrapposti.

[31] CEDU, ric. 24029/07 (2012). Nel 2000 la ricorrente era stata arrestata dalla polizia dopo essere scomparsa per un giorno con suo nipote nel tentativo di impedire la sua partenza in Australia a seguito della rottura del matrimonio di suo figlio. Le autorità hanno deciso di non procedere penalmente e lei è stata invece ammonita per rapimento di minori. La misura di ammonimento inizialmente era destinata a rimanere nel suo registro per cinque anni, ma a causa di un cambio di politica nei casi in cui la parte lesa fosse una bambina, quel periodo è stato successivamente esteso alla vita. La ricorrente si è lamentata della conservazione a tempo indeterminato e della divulgazione del suo ammonimento e dell'impatto di ciò sulle sue prospettive di impiego.

[32] CEDU, ric. 21010/10.

[33] CEDU, ric. 45245/15.

La Corte ha sottolineato in particolare che non era stata la durata della conservazione dei dati a essere stata determinante, ma l'assenza di alcune garanzie. Nel caso del richiedente, i suoi dati personali erano stati conservati a tempo indeterminato senza tener conto della gravità del suo reato, della necessità di una conservazione indefinita e senza alcuna reale possibilità di revisione. Notando anche che la tecnologia utilizzata si è dimostrata più sofisticata di quella considerata dai tribunali nazionali in questo caso, in particolare per quanto riguarda la conservazione e l'analisi delle fotografie, la Corte ha ritenuto che la conservazione dei dati del richiedente non fosse riuscita a trovare un giusto equilibrio tra gli interessi pubblici e privati concorrenti.
Pur con le dovute differenze, può ricavarsi un principio comune e unificante da queste pronunce: esse impongono un rapporto di ragionevole proporzionalità tra la misura della pubblica autorità di conservazione e trattamento dei dati giudiziari, l'impatto che essa determina sulla ampia sfera di vita privata della persona, e gli scopi legittimi perseguiti.

5. Conclusioni

In ultima analisi, si può affermare come il diritto alla riservatezza sia riconosciuto e tutelato dagli artt. 2, 14, 15 Cost., 8 CEDU, 7 e 8 e 52 CDFUE, dai quali si trae un modello di garanzie pari a quello delineato dallo statuto costituzionale interno con riferimento ai diritti di libertà classici: i diritti fondamentali possono essere limitati soltanto nel rispetto di una riserva di legge chiara ed accessibile e di un atto motivato dell'autorità giudiziaria, alla luce del principio di proporzionalità.
Ognuno vede come la normativa in esame, per tutte le ragioni sopra ampiamente svolte, non preveda le garanzie richieste dalla normativa costituzionale ed europea: ossia regole chiare e dettagliate, non dotate peraltro dei requisiti di sufficiente accessibilità e precisione in ordine al trattamento dei dati giudiziari oggetto del collegamento da remoto, affidando di volta in volta all'autorità procedente la scelta di procedere da remoto.
Inoltre, la normativa in esame, dettata sull'onda dell'emergenza, non ha previsto alcuna altra specificazione in ordine alle procedure da seguire per la conservazione dell'integrità del dato giudiziario, l'accesso, l'esame, l'uso, la comunicazione e la cancellazione dei dati giudiziari oggetto di trasmissione telematica entro i tempi di stretta necessità dell'emergenza, in modo da realizzare la cosiddetta minimizzazione dei dati.
In definitiva, risulterebbe assente uno statuto di questo trattamento speciale di dati operato con modalità automatizzate, avendo obliterato altresì il legislatore una valutazione dei rischi aggiuntivi che tale modalità pone rispetto all'ordinario trattamento di dati che avviene in sede processuale.
Non ci pare, infine, che i più recenti sviluppi in materia, e in particolare il parere positivo espresso dal Garante per la protezione dei dati personali in merito al cd. processo amministrativo da remoto[34], possano considerarsi idonei a ridimensionare o finanche

[34] Cfr. S. Musco, *Processo da remoto, arriva il via libera del Garante della privacy*, in *Il Dubbio*, 22 maggio 2020; R. Berti - F. Zumerle, *Giustizia digitale, gli aspetti privacy delle udienze da remoto: ecco le regole*, in *agendadigitale.*

a risolvere i molteplici profili problematici sopra enucleati. Non foss'altro perché la natura dei cd. dati giudiziari specificamente afferenti al processo penale, caratterizzata come è da un effetto potenzialmente assai pregiudizievole e stigmatizzante nelle più varie sfere esistenziali della persona[35], impone di confrontarsi con preoccupazioni eccezionali, non comuni a nessun altro ramo dell'ordinamento giuridico.

Conclusivamente, si può dire, che tali preoccupazioni soltanto in parte possano dirsi superate in ragione dell'ultimo intervento del DGSIA che, sebbene non abbia fatto precedere l'emanazione del provvedimento direttoriale da un parere del Garante come invece è stato fatto nel processo amministrativo, ha corretto il tiro emanando in data 21 maggio un nuovo provvedimento con cui riconferma l'utilizzo degli strumenti già individuati nei provvedimenti del 10 e 20 marzo, ma ne precisa il funzionamento e gli aspetti privacy. In particolare si precisa che mentre i dati delle videoudienze attraverso *Microsoft Teams* sono ospitati su server di Microsoft in Irlanda e nei Paesi Bassi (data center che però sono "amministrati dalla D.G.S.I.A."), i dati relativi alle videoudienze tramite *Skype for Business* sono ospitati direttamente in data center dell'Amministrazione. Rispetto alle istanze di protezione della riservatezza si precisa che tutti i servizi vengono forniti attraverso un canale di comunicazione criptato. Il Ministero ha puntualizzato, infine, che per quanto riguarda *Teams* e *Skype for Business*, vengono conservati (da Microsoft e su server di Microsoft in Europa, nel caso di *Teams*, o su server del Ministero, nel caso di *Skype*) unicamente i dati tecnici di sessione, quali: orario di inizio e fine sessione, identificativo utente, durata, sistema operativo del dispositivo utilizzato, indirizzo IP[36]. Orbene, permangono distinte perplessità che riguardano comunque il potenziale accesso da parte di Microsoft Corporation ai dati relativi a chat, ai file scambiati nonché ai metadati relativi allo streaming video. Questa problematica è aggravata dal nodo del "*Clarifying Lawful Overseas Use of Data (CLOUD) Act*", che può essere opposto solo in caso di sottoscrizione di appositi *executive agreements* con "*qualifying foreign States*", dal momento che il c.d. "Privacy Shield" tra U.E. e Stati Uniti non sembrerebbe rientrare nel novero di tali *executive agreements*. In altri termini, come già ampiamente esposto, dati particolarmente delicati, attinenti alle vicende giudiziarie di individui incappati negli ingranaggi della macchina processuale, seppur da remoto, verrebbero a subire un trattamento al di fuori dell'alea di controllo di soggetti terzi ed indipendenti, come, invece, richiesto dalla normativa europea, e sarebbero altresì passibili di accessi occulti ed in maniera generalizzata, oltre il limite della stretta necessità, pregiudicando l'integrità e la sicurezza dei dati stessi.

eu, 22 maggio 2020; A. Polito, *Vita pubblica, chi detiene il software?*, in *Corriere della Sera*, 24 maggio 2020.

[35] Cfr. ad es., Cass. pen., sez. II, ord. 25 giugno 2018, n. 29248, nell'interpretare la disposizione di cui all'art. 52, d.lgs. 196/2003, relativo alle condizioni per l'oscuramento dei dati personali nei provvedimenti giurisdizionali penali: «Mentre i «dati sensibili» sono individuati dalla legge [...], lo stesso non può dirsi quanto alla «delicatezza» della vicenda processuale, nozione che necessita di essere riempita di contenuti concreti, sintomatici della peculiarità del caso e della capacità, insita nella diffusione dei dati relativi, di riverberare – come osserva lo stesso Garante – «negative conseguenze sui vari aspetti della vita sociale e di relazione dell'interessato (ad esempio, in ambito familiare o lavorativo)», così andando ad incidere pesantemente sul diritto alla riservatezza del singolo". Conseguentemente non basta, per ottenere l'oscuramento, il "danno alla reputazione", perché, altrimenti, "ogni processo penale dovrebbe comportare l'oscuramento dei dati personali».

[36] Cfr. *amplius* in proposito, R. Berti - F. Zumerle, *Giustizia digitale, gli aspetti privacy*, cit.