Risoluzione sul progetto c.d. Active Directory Nazionale.
(Risoluzione del 18 gennaio 2012)

Il Consiglio superiore della magistratura, nella seduta del 18 gennaio 2012, ha adottato la seguente delibera:

" sul progetto c.d. *Active Directory Nazionale*, acquisite le note del Procuratore generale della Repubblica presso la Corte di appello di Venezia, del Presidente della Corte di appello di Venezia, del Procuratore generale della Repubblica presso la Corte di appello di Brescia, del Procuratore della Repubblica presso il Tribunale di Vibo Valentia, del Presidente del Tribunale di Milano e del Procuratore della Repubblica presso il Tribunale di Milano, osserva quanto segue.

1. - Le questioni sollevate dagli uffici giudiziari.

Con nota in data 22 dicembre 2010, indirizzata al Consiglio superiore della magistratura e, per conoscenza, al Ministero della giustizia, Direzione Generale per i Sistemi Informativi Automatizzati (D.G.S.I.A.), ai Procuratori presso i Tribunali del distretto di Venezia ed al Presidente della Corte di appello di Venezia, il Procuratore generale della Repubblica presso la Corte di appello di Venezia ha chiesto che il Consiglio si esprima "*sulla compatibilità del progetto Active Directory Nazionale con i principi e le norme che regolano la giurisdizione*".

In particolare, il suddetto Dirigente, a seguito di una riunione di coordinamento con i Procuratori del distretto espressasi in senso conforme, ha sollevato la questione in riferimento alla comunicazione del dirigente del Coordinamento Interdistrettuale per i Sistemi Informativi Automatizzati (C.I.S.I.A.) di Padova circa l'avvio delle operazioni di migrazione in sede centrale dei dati contenuti nei *server* di ciascun ufficio e ciò proprio in attuazione del progetto *Active Directory Nazionale*; l'attuazione di tale progetto, secondo quanto si legge nella nota del Procuratore generale, comporterebbe che *<<le risorse informatiche interne a ciascuno ufficio, ivi compresi gli applicativi quali Re.ge., saranno gestite da una "struttura gerarchica centralizzata alla quale affidare le informazioni relative a tutti i sistemi e servizi informatici dell'organizzazione", posta in grado, quindi, di effettuare non solo operazioni di controllo ma anche di gestione dei dati>>*, in violazione dei principi costituzionali dell'autonomia della giurisdizione e del codice della *privacy*, dal momento che consentirebbe *<<all'autorità amministrativa di accedere, conoscere e gestire dati personali e giudiziari che devono essere custoditi e controllati dal solo ufficio giudiziario che ne dispone, presso il quale si trovano gli esclusivi titolare e responsabile del trattamento degli stessi (artt. 28 e 29 del D.Lgs. 30/6/2003, n. 196>>*, principi applicabili senza distinzione ai dati giudiziari in materia penale e civile.

Con nota in data 20 gennaio 2011, indirizzata al Consiglio superiore della magistratura, al Ministero della giustizia - D.G.S.I.A. - ed al Procuratore generale presso la Corte di appello di Venezia, il Presidente della Corte di appello di Venezia ha comunicato che il locale Consiglio giudiziario, nella seduta del 19 gennaio 2011, si è espresso in ordine alla nota del 22 dicembre 2010 sopra citata, chiedendo che il CSM esamini la pratica anche con riferimento ai dati gestiti dagli uffici giudicanti.

Con nota in data 26 gennaio 2011, indirizzata al Consiglio superiore della magistratura, il Procuratore generale della Repubblica presso la Corte di appello di Brescia ha rappresentato che, a seguito della riunione dei Procuratori del distretto, è stato deciso di proporre un quesito negli stessi termini di quello formulato dal Procuratore generale di Venezia in data 22 dicembre 2010.

Con nota in data 23 marzo 2011, indirizzata al Presidente della Settima Commissione del Consiglio superiore della magistratura, il Procuratore della Repubblica presso il Tribunale di Vibo Valentia ha rappresentato che i Procuratori del distretto di Catanzaro hanno richiesto al Procuratore generale una riunione per discutere delle problematiche sollevate con riferimento al progetto *Active Directory Nazionale*, in relazione ad una allegata nota DGSIA, datata 28 aprile 2010, dalla quale emergerebbe che la *<<migrazione dei server in un unico dominio di fatto consentirà all'amministratore del sistema non solo di accedere ai dati degli applicativi informatici in un uso (in particolare a quelli del registro informatico RE.GE.), ma anche a tutti i dati e ai documenti*

presenti nella workstation", aggiungendosi altresì che "*il tutto avverrà da remoto senza che sia possibile esperire alcun controllo*"*>>*.
Con nota in data 24 marzo 2011, indirizzata al Consiglio superiore della magistratura, il Presidente del Tribunale ordinario di Milano ed il Procuratore della Repubblica presso il medesimo Tribunale hanno formulato lo stesso quesito già avanzato dal Procuratore generale presso la Corte di appello di Venezia.
In particolare, i citati Dirigenti, premesso il carteggio intercorso sul tema con la DGSIA e precisato che, con nota del 3 dicembre 2010, non si era dato corso alla migrazione verso l'infrastruttura *Active Directory Nazionale* per non aver ricevuto adeguate informazioni e garanzie circa la sicurezza del sistema in questione, hanno evidenziato alcuni aspetti di criticità del progetto, incentrati nella *<<mancanza di una piena ed effettiva separazione dei dati attinenti alla attività giurisdizionale da quelli attinenti alla mera conduzione e manutenzione delle postazioni di lavoro (oltre che dei server interessati dal sistema ADN)>>*.
Hanno, altresì, sottolineato la delicatezza ed importanza della problematica relativa all'accesso dei dati residenti nei *personal computer* connessi alla rete giustizia - tanto più ove la postazione di lavoro sia abilitata anche all'accesso al registro penale informatizzato - richiamando da un lato le specifiche competenze attribuite ai magistrati referenti per l'informatica dalla risoluzione consiliare del 7 giugno 2000, dall'altro il disposto di cui all'art. 4, comma 1, lett. f), d.lgs. 196/2003, che assegna al titolare dei dati giudiziari - da individuare, quanto ai dati relativi alle indagini preliminari, nel Procuratore della Repubblica - *<<le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza>>*.
Sulla base di tali presupposti, nella nota in commento è stata prospettata la necessità di interpretare l'obbligo di leale collaborazione tra Autorità giudiziaria e Ministero della giustizia sul tema dell'informatizzazione, di cui all'art. 1 *bis* d.lgs. 25 luglio 2006 n. 240, così come modificato dalla legge 22 febbraio 2010 n. 24 (in base al quale "*il magistrato capo dell'ufficio giudiziario deve assicurare la tempestiva adozione dei programmi per l'informatizzazione predisposti dal Ministero della giustizia per l'organizzazione dei servizi giudiziari*") in conformità ai principi generali sulla tutela del dato giurisdizionale, con particolare riferimento ai dati coperti dal segreto di indagine (concernente non solo le postazioni del pubblico ministero ma anche quelle dell'ufficio del giudice per le indagini preliminari).

2. – <u>La posizione del Ministero - D.G.S.I.A.</u>

Con nota in data 2 marzo 2011, indirizzata al Consiglio superiore della magistratura e, per conoscenza, al Capo Dipartimento dell'organizzazione giudiziaria, il Direttore generale SIA ha riscontrato la nota del Procuratore generale di Venezia, fornendo alcuni chiarimenti e richiamando, per il resto, la corrispondenza intercorsa con gli uffici giudiziari, pure trasmessa in allegato.
In sintesi, il Direttore generale ha rappresentato che il progetto informatico in questione, peraltro già distribuito ad oltre 20.000 utenti, *<<costituisce un'infrastruttura essenziale per il corretto funzionamento del sistema informativo della giustizia, ed è ritenuta - dalla competente autorità per l'informatica - perfettamente aderente agli standard tecnologici e normativi vigenti>>*.
Sul punto specifico in contestazione, concernente la possibilità (ed il correlativo rischio) di indebiti accessi ai dati giudiziari, nella nota viene chiarito che l'infrastruttura tecnica *<<non consente in alcun modo agli amministratori della stessa di conoscere e utilizzare le credenziali di accesso dei singoli utenti, né di accedere da remoto alle postazioni di lavoro>>*; si aggiunge, altresì, che *<<il sistema di autenticazione ha riguardo soltanto alle procedure per l'accesso al dominio giustizia e non anche alle applicazioni; l'accesso a dette applicazioni (tra cui, in particolare, i sistemi di gestione informatizzata dei registri generali) rimane regolato dalle profilature specifiche che prevedono un utente e password, a disposizione del singolo utente e dallo stesso custodita.>>*.
In questo senso, si specifica che *<<la principale innovazione del nuovo sistema di autenticazione nazionale consiste nella unificazione in un unico dominio di tutti gli utenti della giustizia, ciò al fine di evitare il proliferare di utenze personali distribuite sul territorio in maniera incontrollata e*

indipendentemente dalla persistenza di permanenza del soggetto nell'ambito dell'organizzazione giudiziaria.>>

Fra gli allegati inviati dal Direttore generale SIA è utile evidenziare:

- la nota datata 10 dicembre 2010, con la quale il Direttore generale SIA ha riscontrato direttamente la nota del Procuratore generale della Corte di appello di Venezia, fornendo i seguenti chiarimenti: 1) quanto alla separazione dei dati attinenti alla attività giurisdizionale da quelli attinenti alla mera conduzione e manutenzione delle postazioni di lavoro e dei *server*, si precisa che la sicurezza dei dati "*va garantita anche e soprattutto dall'applicativo e dal database ad esso collegato*", onde la riservatezza del dato - se garantita dall'applicativo - rimane assicurata sia dall'eventuale intrusione dell'amministratore locale del *server* che dall'amministratore del dominio nazionale; 2) quanto alla tracciatura degli accessi, di cui ai requisiti richiesti dal Garante per la protezione dei dati personali con provvedimento del 27 novembre 2008, si rappresenta che è in corso di approntamento un sistema di *event and log management* per la raccolta e la normalizzazione sia dei *log* di accesso ai sistemi *server* o di rete sia degli *alert* per l'analisi e la correlazione degli eventi di sicurezza, ma che tale sistema più avanzato di protezione sarà disponibile solo per le postazioni di lavoro attestate sul dominio *Active Directory Nazionale;* 3) quanto alla competenza in materia di politiche di gestione degli accessi ai sistemi informatici da parte degli utenti dell'amministrazione della giustizia, è stato richiamato l'art. 46 del d.lgs. n. 196/2003 circa la titolarità del trattamento dei dati in ambito giudiziario rispettivamente in capo agli uffici giudiziari ed al Ministero della giustizia, ciascuno nell'ambito delle rispettive competenze, per evidenziare che i diversi livelli di responsabilità devono concorrere alla definizione dei profili di autorizzazione da rilasciare ai singoli utenti del sistema; in tal modo, è stato chiarito che mentre l'utente viene autenticato all'accesso al dominio giustizia tramite l'infrastruttura *Active Directory Nazionale*, per assicurare l'attuale appartenenza del singolo utente all'amministrazione della giustizia (*ex* art. 8, comma 1, d.m. 27 aprile 2009, "*nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia*"), le specifiche autorizzazioni all'accesso alle varie applicazioni (come ad esempio il sistema re.ge.), sono di competenza dei titolari dei dati e quindi dei responsabili degli uffici giudiziari, i quali sono tenuti, direttamente o a mezzo degli ADSI opportunamente a ciò delegati (art. 4) a definire le politiche di accesso alle applicazioni ai dati (art. 8, comma 3). Pertanto, "*l'introduzione dell'autenticazione tramite ADN non modifica in alcun modo le procedure di autorizzazione dei singoli utenti all'accesso alle singole applicazioni: l'esistenza di una utenza ADN è il presupposto per accedere alle applicazioni della giustizia, ma il concreto accesso alla singola applicazione (ad esempio re.ge.) è regolato dagli specifici profili di autorizzazione di tale software.*". In proposito, si aggiunge che <<*per garantire la necessaria autonomia degli uffici giudiziari nella gestione delle politiche di accesso ai dati ed alle applicazioni, è stabilito (art. 8, comma 6) che "la struttura per la sicurezza del distretto individua i referenti degli uffici per l'assegnazione agli utenti dei profili relativi al trattamento dei dati". La struttura per la sicurezza, definita (art. 1) quale "organizzazione per la sicurezza informatica degli uffici giudiziari del distretto", può giovarsi, nell'ambito delle prerogative del Procuratore generale della Corte d'appello in tema di sicurezza, del personale informatico collocato nella pianta organica degli uffici giudiziari di Procura Generale, proprio allo scopo di fornire supporto tecnico alla gestione delle utenze e dei profili degli utenti abilitati al trattamento dei dati*>>;
- la nota datata 16 dicembre 2010, sempre indirizzata al Procuratore generale presso la Corte di appello di Venezia, con la quale il Direttore generale SIA ha ribadito che "*le password di accesso nominative degli utenti sono in possesso solo ed unicamente di questi ultimi e che l'accesso ai dati dei registri avviene per il tramite degli applicativi che già oggi svolgono*

tale attività con piena soddisfazione degli uffici", esprimendo comunque la disponibilità ad eventuali approfondimenti di carattere tecnico;

- la nota datata 2 novembre 2010, indirizzata al Procuratore generale presso la Corte di appello di Milano, nella quale il Direttore generale SIA, nel richiamare il disposto di cui all'art. 8, comma 1, d.m. 27 aprile 2009 in ordine alla competenza del Responsabile SIA in materia di politica di gestione degli accessi da parte degli utenti dell'amministrazione della giustizia, con assegnazione agli amministratori dei servizi informatici (ADSI) di uno o più profili volti alla conduzione, anche remota, dei sistemi e delle postazioni di lavoro, precisa che l'architettura del sistema, a struttura gerarchica, consente la possibilità di approntare *<<infrastrutture tecniche locali (site ADN) che replicano quelle centrali e rendono in certo modo "federale" il sistema>>*; tale soluzione, indicata come idonea a "*consentire una maggiore efficienza e capacità di controllo locale da parte di uffici di particolare rilevanza*", è prevista per gli uffici di Milano, con attivazione presso le realizzande strutture del locale CISIA. In proposito, si precisa che la struttura organizzativa ricalcherà l'architettura del sistema, con la nomina di amministratori centrali presso la DGSIA, nominati dal Responsabile SIA, e di delegati locali, nominati dal Direttore del CISIA competente. Infine, quanto alla tracciatura degli accessi, viene precisato che i CISIA mantengono un apposito registro con i nominativi dei tecnici delle ditte esterne autorizzate all'accesso e per i quali è stato creato un *account* nominativo; inoltre, i *log* relativi agli accessi ed alle attività compiute sulle postazioni di lavoro sono conservati all'interno di appositi *file* nelle medesime postazioni di lavoro, accessibili agli amministratori locali, con possibilità di prevedere l'esportazione automatica dei *log* e la loro conservazione in un sito protetto;
- nota datata 13 dicembre 2010, sempre indirizzata ai Dirigenti degli uffici di Milano, con la quale il Direttore generale SIA ha ulteriormente precisato che il dominio *Active Directory Nazionale* aggiunge un livello, quello degli amministratori di dominio nazionale, nominati dal Direttore Generale e comunicati agli uffici, amministratori che assumono i medesimi doveri degli ADSI locali, consentendo vantaggi sul piano della razionalizzazione degli accessi ai servizi già forniti secondo una logica di autenticazione unica ed integrata, con possibilità di tracciare gli accessi ai sistemi, censimento delle postazioni e dei *server*, monitoraggio centralizzato della distribuzione degli aggiornamenti dei sistemi operativi e della piattaforma antivirus;
- parere rilasciato dal CNIPA al Ministero della giustizia (parere 67/05 del 5.5.2005), dal quale emerge che ADN è una "*infrastruttura di autenticazione Window 2003*"; il parere del CNIPA - reso a richiesta del Ministero - ha ad oggetto la congruità tecnico–economica del contratto in via di perfezionamento tra il Ministero e Microsoft per il dispiegamento della suddetta infrastruttura e l'addestramento del personale tecnico. La stipula di detto contratto si inseriva in un complesso progetto ministeriale avente tra i suoi obiettivi, per quanto qui interessa, la ridefinizione dell'architettura di dominio. Il parere del CNIPA è favorevole alla stipula (a pag. 8 del parere si legge: "*L'iniziativa in questione, che si inserisce nelle linee di interventi previste nell'ambito delle politiche di sicurezza che il Ministero ha in corso di realizzazione, è da considerarsi condivisibile*"), con alcune osservazioni (relative al *mix* di figure professionali messo a disposizione da Microsoft e, quindi, all'entità del corrispettivo contrattuale) che non toccano le questioni rilevanti nella presente sede.

In seguito a parere espresso sulla questione dal proprio organo ausiliario Struttura Tecnica per l'Organizzazione (STO), la Settima Commissione Referente, tramite il tavolo tecnico CSM – Ministero della giustizia, ha avviato una prima interlocuzione con la DGSIA, dovendo essere approfonditi una serie di aspetti:

- ✓ eventuale adozione di *policy* sicurezza ulteriori rispetto a quanto indicato nella nota 28.4.2010, in attuazione del d.m. 2009, con particolare riferimento alla nomina degli ADSI, alla eventuale interazione con gli uffici in proposito alle procedure di

monitoraggio, ove del caso, in diretta relazione alla implementazione del progetto ADN;

- ✓ stato di diffusione del progetto ADN, con indicazione della geografia della distribuzione, e delle concrete implementazioni adottate rispetto alla precedente architettura tecnologica ed organizzativa, nonché dell'eventuale adozione di configurazioni differenti per specifici distretti (in particolare, chiarimenti sulle politiche di dispiegamento ed implementazione con riferimento alla enunciata scelta di "*site ADN*", come indicato nelle note di riscontro ai Dirigenti degli uffici di Milano).

Con nota del 4 ottobre 2011 il Direttore Generale S.I.A. ha riscontrato solo parzialmente le richieste di approfondimento istruttorio, giacché non è stata fornita alcuna specifica indicazione circa l'adozione, in attuazione del d.m. 2009, di *policy* sicurezza ulteriori rispetto a quanto indicato nella nota 28 aprile 2010.

Ci si riferisce, in particolare, ai criteri di nomina degli ADSI ed alle modalità della eventuale interazione con gli uffici nella implementazione del progetto ADN; nonché alla descrizione dello stato di diffusione del progetto ADN (con indicazione della geografia della distribuzione e delle concrete implementazioni adottate, tenuto anche conto della enunciata scelta di adottare per alcuni uffici una logica articolata a livello territoriale e denominata "*site ADN*", come indicato nelle note di riscontro ai Dirigenti degli uffici di Milano).

E' tuttavia abbastanza chiara la precisazione che la competente articolazione ministeriale ha fornito in ordine alla organizzazione interna degli amministratori, articolata in due aree di competenze (una dedicata alla gestione delle applicazioni ed una dedicata alla gestione delle utenze), ognuna delle quali è strutturata su diversi divelli gerarchici (area principale, o dominio, articolata in unità organizzative di primo livello, a loro volta strutturate in altre unità organizzative).

In tale organizzazione le aree sono gestite da amministratori nazionali, mentre le unità organizzative di primo livello (che nell'area dedicata alla gestione utenti corrispondono ad Uffici centrali del Ministero, Dipartimenti o Distretti giudiziari) sono gestite da amministratori nominati dalla D.G.S.I.A. che, a loro volta, possono delegare le attività di competenza ad altri amministratori di sistema, mantenendo tuttavia la possibilità di operare direttamente.

I delegati di distretto sono normalmente tre per distretto di Corte di appello e sono nominati dai dirigenti CISIA nell'ambito del personale informatico in servizio presso il medesimo Coordinamento Interdistrettuale, tenendo conto della professionalità, dell'affidabilità e del rapporto fiduciario con gli uffici giudiziari. In esito a tali chiarimenti la Direzione ha trasmesso l'elenco nominativo degli amministratori di livello nazionale e per i diversi distretti giudiziari.

3. - <u>Quadro normativo di riferimento e considerazioni.</u>

La questione, nei termini in cui è stata prospettata dai citati uffici giudiziari, si appalesa senz'altro di estrema delicatezza.

In sintesi, il Procuratore generale di Venezia ha revocato in dubbio la compatibilità del progetto *Active Directory Nazionale* sul presupposto che esso consentirebbe all'autorità amministrativa l'accesso ai dati giudiziari, in contrasto con i principi costituzionali in materia di giurisdizione oltre che con il codice di protezione dei dati personali.

Sulla medesima linea si collocano le posizioni del Presidente della Corte di appello di Venezia, in qualità di Presidente del locale Consiglio giudiziario, del Procuratore generale presso la Corte di appello di Brescia e del Procuratore della Repubblica presso il Tribunale di Vibo Valentia.

Di più ampio respiro, invece, nonostante l'identità del quesito formulato, la posizione dei Dirigenti degli uffici milanesi, i quali hanno prospettato l'emergente questione relativa al progetto *Active Directory Nazionale* nel più ampio quadro delle relazioni istituzionali e della leale collaborazione che deve informare lo sviluppo della informatica nel settore della giustizia.

La DGSIA, dal canto suo, ha chiarito che il progetto denominato *Active Directory Nazionale* si basa sull'adozione della tecnologia *Microsoft Active Directory* quale tecnologia scelta dall'amministrazione per costruire il proprio sistema di *directory* (i.e. "elenco"), con ciò intendendo

la creazione di una "*struttura centralizzata e gerarchica cui affidare la conoscenza di tutte le risorse dell'intera organizzazione (utenti, servizi, programmi, server, client, ecc.) ed attraverso la quale, con opportuni strumenti, effettuare operazioni di controllo e gestione delle stesse.*"
La scelta viene motivata dall'amministrazione su un piano tecnico come scelta coerente rispetto alla consolidata utilizzazione della tecnologia Microsoft e come esigenza di razionalizzazione della politica di gestione dei sistemi di autenticazione al dominio giustizia secondo *policy* di centralizzazione, per prevenire inadeguatezze scontate a livello locale (nella nota DGSIA 2 marzo 2011 si menzionano espressamente casi di proliferazione di utenze personali distribuite sul territorio in maniera incontrollata ed indipendentemente dalla persistente permanenza del soggetto nell'ambito dell'organizzazione giudiziaria).
Sotto altro profilo, la scelta viene motivata anche in base a logiche di efficienza dell'organizzazione e della gestione delle risorse informatiche, attraverso la gestione unificata del sistema degli accessi, cioè delle credenziali di autenticazione (*username/password*), che diventeranno uniche per tutti i servizi cui si ha diritto di accedere secondo la specifica profilatura (SSO -*Single Sign One*).
Va, peraltro, evidenziato che l'articolazione ministeriale rivendica la diretta responsabilità delle politiche di accesso, secondo il nuovo regolamento 27 aprile 2009, e la discrezionalità tecnica nell'attuazione, nel rispetto dell'esclusiva titolarità dei dati giudiziari in capo ai Dirigenti degli uffici.

3a. - Tanto premesso è utile chiarire il **quadro normativo di riferimento** richiamato nelle note sopra citate.
Gli uffici giudiziari si richiamano essenzialmente, oltre ai principi costituzionali ed alla normativa codicistica, soprattutto in materia penale, al d.lgs. 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali (c.d. codice della *privacy*), ed individuano il titolare del dato giudiziario nel dirigente dell'ufficio. In particolare, il Procuratore generale presso la Corte di appello di Venezia ha richiamato gli artt. 28 e 29 del codice, rispettivamente in tema di titolare del trattamento (art. 28: "*Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.*") e responsabile del trattamento (art. 29: "*1. Il responsabile è designato dal titolare facoltativamente. 2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. 3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. 4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare. 5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.*").
Il Direttore SIA ha, invece, richiamato l'art. 46 del codice *privacy* in tema di trattamenti in ambito di giudiziario (art. 46: "*1. Gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento. 2. Con decreto del Ministro della Giustizia sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, relativamente a banche di dati centrali od oggetto di interconnessione tra più uffici o titolari. I provvedimenti con cui il Consiglio superiore della magistratura e gli altri organi di autogoverno di cui al comma 1 individuano i medesimi trattamenti da essi effettuati sono riportati nell'allegato C) con decreto del Ministro della Giustizia.*", segnalando la concorrenza delle attribuzioni secondo le rispettive competenze istituzionali.

Inoltre, il Direttore generale SIA, anche in qualità di responsabile SIA, richiama (e presuppone) le disposizioni di cui al d.m. 27 aprile 2009 - "*Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia*".
Attesa la delicatezza del tema, appare opportuno riportare alcuni passaggi essenziali di tale decreto, che assumono rilievo per la migliore comprensione della questione in esame.
Il decreto fissa, in sostituzione del decreto ministeriale 24 maggio 2001, le regole procedurali per la gestione del sistema informatico del Ministero della giustizia e per la tenuta informatizzata dei registri tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari (art. 1). Le regole procedurali per la tenuta dei registri informatizzati, contenute nell'allegato tecnico, stabiliscono le caratteristiche del sistema informatico (art. 2 allegato) in termini di disponibilità ("*i dati sono formati, raccolti, conservati, resi disponibili e accessibili in modo da assicurarne l'uso interno e la fruizione, anche in caso di eventi interruttivi del funzionamento dei sistemi, compatibilmente con i livelli di servizio prestabiliti*"), integrità ("*i dati sono trattati in modo da assicurarne precisione, completezza e inalterabilità*"), autenticità ("*la provenienza dei dati è garantita e asseverata*") e controllo degli accessi fisici e logici ("*le informazioni possono essere fruite solo ed esclusivamente dalle persone autorizzate a compiere tale operazione*"), nonché l'organizzazione del sistema informatico, articolato a livello nazionale, interdistrettuale, distrettuale e locale (art. 3). La predisposizione ed il periodico aggiornamento delle linee guida per l'organizzazione e la gestione del sistema informatico è a cura del Responsabile SIA (art. 3, comma 7), che provvede, altresì, alla designazione (art. 4, comma 4) degli amministratori dei servizi informatici (ADSI), incaricati di assicurare la conduzione operativa di specifiche componenti del sistema informatico, effettuando, anche mediante accesso remoto, tutte le operazioni necessarie a garantire i requisiti del sistema informatico (art. 4, comma 1).
Gli ADSI vengono individuati fra gli esperti informatici dell'Amministrazione ovvero, se non sono disponibili tali risorse, ricorrendo a personale esterno qualificato (art. 4, comma 4); l'ADSI, se nominato responsabile del trattamento da parte dei titolari delle banche dati, pone in essere le iniziative necessarie per il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri, anche alla luce delle direttive concordemente emanate dai titolari delle banche dati (art. 4, comma 5,); in ogni caso, l'ADSI garantisce che il capo dell'ufficio giudiziario, o un suo delegato, possa accedere alla infrastruttura logistica condivisa per verificare il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri (art. 4, comma 6,).
La D.G.S.I.A produce e mantiene aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informatico (art. 5, comma 1) e l'ADSI predispone un dettagliato inventario delle componenti del sistema informatico di sua competenza (art. 5, comma 3) e lo mantiene aggiornato ogni qualvolta si verifica una variazione; l'inventario è reso disponibile a tutti gli uffici interessati.
Quanto alla gestione della sicurezza del sistema informativo, è stabilito che il Responsabile S.I.A. predispone il documento programmatico della sicurezza di cui all'art. 34 del d.lgs. 30 giugno 2003 n. 196, relativamente alle componenti del sistema informatico dell'Amministrazione, che sono centralmente gestite e controllate (art. 7, comma 1), mentre gli uffici, con la collaborazione tecnica del CISIA competente, predispongono il documento programmatico della sicurezza di cui all'art. 34 del d.lgs 30 giugno 2003 n. 196, relativamente al sistema informativo di propria competenza e lo rendono disponibile al Responsabile S.I.A. (art. 7, comma 2).
La politica di gestione degli accessi è definita e gestita dal Responsabile S.I.A., che individua ed aggiorna periodicamente, con proprio decreto, la procedura di autenticazione (art. 8); ogni utente ottiene, tramite la procedura di autorizzazione, uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo di autorizzazione, rispetto alle risorse del sistema informatico (art. 8, comma 3).
E', però, stabilito che l'assegnazione agli utenti dei profili relativi al trattamento dei dati è attribuita ai referenti degli uffici individuati dalla struttura per la sicurezza del distretto (art. 8, comma 6). Le attività relative all'utilizzo e alla gestione del sistema informatico, anche da remoto, sono sottoposte ad un processo continuo di controllo e verifica della loro corretta e completa esecuzione (art. 10,

comma 1); per questo, il sistema informatico prevede, a garanzia della autenticità e della integrità dei dati e come misura minima di monitoraggio, la registrazione di tutti gli accessi, anche di carattere tecnico, ivi compresi quelli non riusciti o falliti, e di tutte le operazioni effettuate sui dati (art. 10, comma 2,); la responsabilità del corretto svolgimento di tali attività è rimessa alla D.G.S.I.A., anche se affidate a personale esterno specificamente individuato (art. 10, comma 3).
Le registrazioni dei *log* delle attività di monitoraggio devono essere trascritte con cadenza almeno settimanale su supporti non riscrivibili da conservare unitamente ai *backup* (art. 10, comma 4) e la struttura per la sicurezza del distretto, i titolari ed i responsabili per il trattamento dei dati hanno facoltà di esaminare, nell'ambito delle rispettive competenze, le predette registrazioni (art. 10, comma 5); tutte le operazioni di manutenzione effettuate sui dati sono soggette ad autorizzazione e registrazione (art. 13, comma 2).
Infine, si attribuisce al Responsabile S.I.A. la definizione della politica della sicurezza dei sistemi informatici della giustizia (art. 15), attraverso l'adozione di un decreto che preveda, fra l'altro, le linee guida relative a: a) modalità di gestione delle utenze; b) modalità di comportamento delle utenze agli effetti della sicurezza informatica; c) controllo fisico e logico degli accessi ai sistemi informatici; d) politiche, modalità esecutive e strumenti per la salvaguardia dei dati (*backup*, *disaster recovery*, ecc.); e) politiche e modalità esecutive per la conservazione e la riproduzione dei supporti fisici dei dati; f) gestione dei sistemi di protezione dagli attacchi informatici (antivirus, antispam, firewall, IDS, IPS, ecc); g) modalità e strumenti di supporto per il controllo e il monitoraggio della sicurezza informatica; h) procedure di verifica e controllo dei livelli di sicurezza informatica; i) politiche per la formazione degli utenti in tema di sicurezza informatica.

3b. - Così chiarito il quadro normativo di riferimento, si ritiene che la questione prospettata non debba tanto essere considerata con riferimento alla specifica tecnologia utilizzata ed in contestazione (tecnologia Microsoft *Active Directory*), bensì con riferimento alla concreta implementazione della stessa in relazione alle politiche di sicurezza dei sistemi informatici.
Sul punto, infatti, è interessante porre in evidenza il contenuto della nota del Direttore generale SIA in data 28 aprile 2010, relativa alle *policy* di sicurezza dei sistemi informatici e trasmessa in allegato alla nota del Procuratore della Repubblica presso il Tribunale di Vibo Valentia; con tale nota, si prevede la necessità di ridefinire in appositi provvedimenti del Responsabile SIA le *policy* di sicurezza conseguenti all'entrata in vigore del d.m. 27 aprile 2009, reputando opportuno, nelle more, mantenere le misure minimali già indicate nel d.m. 24 maggio 2001.
Rispetto a tali misure, nella citata nota, si richiamano alcune prescrizioni, fra le quali si ritiene di evidenziare le seguenti:

a) ad ogni *workstation* è assegnato un utente al quale è associato un profilo con privilegi di accesso e utilizzo delle risorse del sistema informatico concessogli dal responsabile del trattamento dei dati;
b) ad ogni utente è assegnata una credenziale specifica di autenticazione al proprio profilo onde garantire l'accesso ai soli dati e risorse necessari per l'espletamento delle operazioni di propria competenza;
c) nessun utente è abilitato a modificare autonomamente i privilegi del proprio profilo e quindi nessun utente può avere a disposizione una utenza con privilegi di tipo amministrativo;
d) ogni operazione inerente alla gestione delle postazioni di lavoro è attribuita alla competenza di un gruppo di amministratori di sistema tutti nominativamente individuati nel documento programmatico della sicurezza;
e) "*la possibilità di disabilitare totalmente l'accesso alle ridette risorse informatiche (pdl critiche) per gli utenti amministratori - seppur tecnicamente ipotizzabile - sarebbe in contrasto con il principio di cui al precedente punto 2 e non conforme alla ratio delle disposizioni vigenti; ferme le conseguenze organizzative scaturenti da tali politiche di sicurezza in merito all'inibizione per i tecnici informatici di prestare assistenza sulle postazioni di lavoro. Per tale ragione possono far parte del gruppo di Administrator delle workstation anche i sistemisti esterni incaricati del servizio di assistenza. Tutte le risorse*

informatiche e la loro potenziale condivisione fra gli utenti, grazie alla rete, sono inoltre governate nell'ambito di un dominio. La conduzione del dominio è affidata ad uno o più amministratori. Tali amministratori di dominio potranno utilizzare, tra le altre, le funzionalità "hidden administrative shares" (condivisione amministrativa nascosta) e "desktop remoto" non disabilitate per le ragioni di cui al punto 3. Tutti gli accessi sia lato server che lato client - alle risorse informatiche vengono registrati in appositi file di log utilizzando gli strumenti sw posti a disposizione dei sistemi Microsoft Windows.".

Rispetto a quelle descritte viene espressamente rappresentato che "*le misure suindicate non possono escludere che l'utente Administrator possa accedere ai dati e documenti presenti sulla workstation perché, come già evidenziato, la stessa architettura logica dei sistemi Windows prevede che uno o più utenti individuati come Administrator abbiano la prerogativa di amministrare i sistemi nella loro totalità.*"

Avuto riguardo al contenuto di tale nota, il Direttore generale SIA ha chiarito che il sistema ADN si limita ad aggiungere un livello di amministratori a livello nazionale rispetto agli attuali ADSI locali, reputando che l'adozione di tale infrastruttura tecnologica e delle conseguenti misure organizzative valga a rendere maggiori servizi, anche sul piano della sicurezza, consentendo nel contempo una maggiore efficienza complessiva del sistema.

Parrebbe, dunque, doversi concludere che non è tanto la scelta del progetto *Active Directory Nazionale* in sé a dover essere considerata quanto la sua concreta implementazione con riferimento alle politiche di sicurezza; in altri termini, non è tanto il livello nazionale o locale di amministratore a comportare rischi per l'indebito accesso ai sistemi, quanto l'adozione di politiche di sicurezza adeguate anche a livello distrettuale, tali da consentire, nel rispetto delle prerogative e delle responsabilità istituzionali, l'efficiente organizzazione dei servizi informatici, divenuti ormai essenziali per il funzionamento degli uffici giudiziari, e la salvaguardia della riservatezza (e, in alcuni casi, segretezza) del dato giudiziario.

In sintesi, il vero nodo critico non sembra direttamente riferibile alla scelta tecnologica del progetto ADN in sé considerata – scelta che può rientrare nella responsabilità tecnica rimessa alla competente struttura ministeriale, che ha individuato i benefici connessi all'attuazione di tale progetto - quanto alla sua concreta implementazione con specifico riferimento all'adozione di adeguate misure di sicurezza.

In particolare, considerato il ruolo cruciale assegnato agli amministratori (ADSI), sia nazionali che locali, è imprescindibile l'adozione di idonee misure di sicurezza con riferimento ai tre passaggi essenziali dei criteri di nomina, della interlocuzione sul punto con gli uffici (tanto più ove occorra avvalersi di fornitori esterni), del monitoraggio degli accessi (in termini di registrazione e conservazione dei *log* su supporti non riscrivibili e non modificabili neppure degli stessi amministratori, oltre che di accessibilità dei risultati del monitoraggio al titolare del trattamento dei dati).

In proposito, va rilevato che nei chiarimenti trasmessi dalla DGSIA non vi sono evidenti riferimenti alla adozione di tali misure, cui, invece, si riferisce la nota trasmessa in allegato alla richiesta del Procuratore di Vibo Valentia; non consta, pertanto, se, in relazione alla introduzione del d.m. 2009 sopra citato ovvero alla diffusione di ADN siano state implementate ulteriori e specifiche misure di sicurezza.

Il quadro normativo di riferimento e gli elementi acquisiti consentono di considerare che la questione prospettata non debba essere considerata con riferimento alla specifica tecnologia utilizzata dalla D.G.S.I.A. per la politica di gestione degli accessi, quanto nel quadro di una leale collaborazione fra la struttura ministeriale e gli uffici giudiziari nella determinazione, ciascuno per quanto di competenza, nell'adozione delle *policy* di sicurezza dei sistemi informatici, con particolare riferimento alla individuazione e nomina degli ADSI, tenuto conto della delicatezza del compito e della loro potenziale duplice veste, anche come responsabile indicato dal titolare del trattamento dei dati giudiziari. In questo senso, la nota integrativa trasmessa dal Direttore Generale S.I.A., con l'indicazione dei nominativi degli amministratori nazionali e dei distretti giudiziari

dell'area gestione utenze, costituisce un'apprezzabile gesto nella linea della trasparenza anche verso l'organo consiliare.

4. – <u>Conclusioni.</u>

In conclusione, si ribadisce che il vero nodo critico non sembra tanto riferibile alla scelta tecnologica del progetto ADN in sé considerata - scelta che può rientrare nella responsabilità tecnica rimessa alla competente struttura ministeriale, che ha individuato i benefici connessi all'attuazione di tale progetto - quanto alla sua concreta implementazione con specifico riferimento all'adozione di adeguate misure di sicurezza.

In particolare, considerato il ruolo cruciale assegnato agli amministratori (ADSI), sia nazionali che locali, è imprescindibile l'adozione di idonee misure di sicurezza con riferimento ai tre passaggi essenziali dei criteri di nomina, della interlocuzione sul punto con gli uffici (tanto più ove occorra avvalersi di fornitori esterni), del monitoraggio degli accessi (in termini di registrazione e conservazione dei *log* su supporti non riscrivibili e non modificabili neppure dagli stessi amministratori, oltre che di accessibilità dei risultati del monitoraggio al titolare del trattamento dei dati).

Infatti, la vicenda relativa all'ADN ha portato a consapevolezza il problema del potenziale accesso ai dati da parte delle strutture ministeriali. Si tratta, tuttavia, di un problema che già preesisteva ed è legato al ruolo stesso degli ADSI, ma che il progetto ADN, con la configurazione di amministratori a livello nazionale, ha reso palese agli uffici giudiziari, i quali hanno conseguentemente ed opportunamente richiesto l'intervento del CSM.

Occorre pertanto rimodulare l'attenzione sullo specifico tema che deve esser oggetto del rapporto di leale collaborazione tra gli uffici e il Ministero, sul quale il CSM può svolgere una efficace opera di coordinamento preventivo, in conformità con l'indirizzo di cui alla recente delibera in data 13 luglio 2011 in tema di "*Ricognizione degli applicativi informatici in uso presso gli uffici giudiziari e verifica delle ricadute della loro utilizzazione sulla produttività e sulla organizzazione degli uffici giudiziari - Ruolo del Consiglio superiore della magistratura rispetto al Piano straordinario per la digitalizzazione preannunciato dal Ministero della giustizia*", nella quale si è evidenziato che l'organo di governo autonomo della magistratura deve istituzionalmente garantire la funzionalità degli uffici giudiziari, collaborando con i loro dirigenti nonché sostenendo ogni misura utile o necessaria per gli interventi di riorganizzazione dei servizi di supporto all'attività giurisdizionale.

Si è a tal riguardo rilevato che il coordinamento delle competenze del Consiglio superiore della magistratura e di quelle del Ministero della giustizia, come sancite rispettivamente dagli artt. 105 e 110 Cost., necessita inevitabilmente di una leale collaborazione istituzionale, proprio ai fini del necessario bilanciamento dei valori costituzionali contenuti nelle citate norme.

Si è, peraltro, precisato che tale collaborazione, per essere reale ed effettiva, deve avvenire in via preventiva ogniqualvolta si tratti di interventi e progetti di riorganizzazione dei servizi informatici ovvero statistici che coinvolgono le competenze e la funzionalità dei servizi giudiziari e giurisdizionali. Solo una preventiva concertazione ed una compiuta informazione sui progetti e gli interventi programmati può infatti consentire un reale coordinamento tra i vari centri di competenza istituzionali che, a vario titolo, assumono quotidianamente determinazioni destinate ad incidere concretamente sulla vita degli uffici giudiziari italiani.

Non si può trascurare, pertanto, in questa sede il problema della tutela dei dati giurisdizionali rapportato al principio di leale collaborazione tra Ministero della giustizia, CSM e uffici giudiziari.

In definitiva si ritiene che, con il ruolo di raccordo del Consiglio superiore della magistratura nell'ambito delle citate competenze di garanzia della funzionalità dell'amministrazione della giustizia, la questione relativa al progetto ADN debba trovare il suo componimento nel quadro di una leale collaborazione fra la struttura ministeriale e gli uffici giudiziari nell'adozione delle *policy* di sicurezza dei sistemi informatici, ciascuno per quanto di competenza e secondo la normativa sopra richiamata, che attribuisce al Responsabile S.I.A. il potere di nomina degli ADSI per lo svolgimento dei compiti loro assegnati, nonché, per altro verso, al titolare delle banche dati (da individuare nel dirigente dell'ufficio giudiziario) la facoltà di nominare il medesimo ADSI come

responsabile del trattamento, anche per l'esecuzione di controlli e verifiche sulla corretta gestione del sistema previsti dagli *standard* di sicurezza adottati.
In ragione di ciò, oltre a proseguire nella interlocuzione con il Ministero – DGSIA, è utile anche un monitoraggio presso gli uffici giudiziari al fine di acquisire una serie di elementi relativi alle politiche di sicurezza fino ad ora adottate per l'accesso ai dati giudiziari, con particolare riferimento alla nomina e comunicazione degli ADSI, ai criteri di assegnazione agli utenti dei profili relativi al trattamento dei dati, al monitoraggio dei dati di sistema ed alla conoscibilità degli esiti del monitoraggio medesimo.
E' utile chiedere, altresì, l'indicazione delle modifiche che sarebbero connesse all'attuazione del nuovo sistema ADN e che indebolirebbero o metterebbero a rischio la sicurezza dei dati.
Sempre al fine di ottenere un quadro conoscitivo soddisfacente, appare opportuno richiedere anche ai magistrati referenti distrettuali per l'informatica (RID) di relazionare sullo stato di attuazione della iniziativa ADN nel distretto di riferimento, con indicazione delle eventuali criticità riscontrate (ovvero dei benefici conseguiti) a seguito della diffusione del sistema.
Tanto premesso, il Consiglio delibera di:
- proseguire nella interlocuzione con il Ministero della giustizia - D.G.S.I.A. onde verificare:
    a) le modalità di coinvolgimento dei dirigenti degli uffici giudiziari nell'adozione di idonee misure di sicurezza con riferimento ai tre passaggi essenziali dei criteri di nomina, della interlocuzione sul punto con gli uffici (tanto più ove occorra avvalersi di fornitori esterni), del monitoraggio degli accessi (in termini di registrazione e conservazione dei *log* su supporti non riscrivibili e non modificabili neppure dagli stessi amministratori, oltre che di accessibilità dei risultati del monitoraggio al titolare del trattamento dei dati);
    b) l' eventuale adozione di *policy* sicurezza ulteriori rispetto a quanto già indicato, in attuazione del d.m. 2009, con particolare riferimento alla nomina degli ADSI, alla eventuale interazione con gli uffici in proposito alle procedure di monitoraggio, ove del caso, in diretta relazione alla implementazione del progetto ADN;
    c) lo stato di diffusione del progetto ADN, con indicazione della geografia della distribuzione, e delle concrete implementazioni adottate rispetto alla precedente architettura tecnologica ed organizzativa, nonché dell'eventuale adozione di configurazioni differenti per specifici distretti (in particolare, chiarimenti sulle politiche di dispiegamento ed implementazione con riferimento alla enunciata scelta di "*site ADN*", come indicato nelle note di riscontro ai Dirigenti degli uffici di Milano);
- richiedere agli uffici giudiziari i seguenti dati:
    1) politiche di sicurezza fino ad ora adottate per l'accesso ai dati giudiziari, con particolare riferimento alla nomina e comunicazione degli ADSI, ai criteri di assegnazione agli utenti dei profili relativi al trattamento dei dati, al monitoraggio dei dati di sistema ed alla conoscibilità degli esiti del monitoraggio medesimo;
    2) indicazione delle modifiche che sarebbero connesse all'attuazione del nuovo sistema ADN e che indebolirebbero o metterebbero a rischio la sicurezza dei dati;
- richiedere ai magistrati referenti distrettuali per l'informatica (RID):
    di relazionare sullo stato di attuazione della iniziativa ADN nel distretto di riferimento, con indicazione delle eventuali criticità riscontrate (ovvero dei benefici conseguiti) a seguito della diffusione del sistema.".