Il processo civile telematico
di Wanda D'Avanzo

Sommario: 1. Introduzione. - 2. Il documento informatico e la firme digitale. - 3. Il dominio giustizia e il sistema informatico civile. - 4. La posta elettronica certificata. - 5. Il fascicolo informatico nel processo telematico. - 6. La tenuta dei registri informatizzati. - 7. La postazione dell'avvocato. - 8. Conclusioni

1. - Il progetto di digitalizzazione del processo costituisce un approccio, nell'ambito dell'amministrazione della giustizia, dei principi relativi all'informatizzazione delle attività della pubblica amministrazione.
L o svolgimento telematico del processo ha trovato la sua prima regolamentazione organica nel DPR del 13 febbraio 2001, n. 123 (Gu n. 89 del 17 aprile 2001), recante la disciplina dell'uso di strumenti informatici e telematici nel processo civile, amministrativo e quello dinanzi alle sezioni giurisdizionali della Corte dei Conti. Le modalità del progetto di automazione del processo sono state, successivamente, descritte nel Decreto Ministeriale del 14 ottobre 2004 (Gu n. 272 del 19 novembre 2004, So 167), recante regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile, e nei suoi allegati, conformemente con quanto previsto dal comma 3 dell'art. 3 del DPR 123/2001.
Il processo telematico ruota intorno a quattro elementi fondamentali. I primi due sono rappresentati dal documento informatico e dalla firma digitale. Ai sensi del primo comma dell'art. 4, DPR 123/2001, "*tutti gli atti e provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale […]*". Qualora non fosse possibile procedere alla sottoscrizione nel modo indicato, gli atti e i provvedimenti saranno "*redatti o stampati su supporto cartaceo, sottoscritti nei modi ordinari e allegati al fascicolo cartaceo*" (art. 4, comma 2).
Gli altri due elementi del processo telematico sono il dominio giustizia e il sistema informatico civile. Per dominio giustizia si intende, *ex* art. 1, lett. e), DPR 123/2001, "*l'insieme delle risorse hardware e software, mediante il quale l'amministrazione della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura*"; il sistema informatico civile, invece, è "*il sottoinsieme delle risorse del dominio giustizia mediante il quale l'amministrazione della giustizia tratta il processo civile*" (art. 1, lett. f).

2. - Il percorso legislativo seguito dalla regolamentazione del documento informatico e della firma digitale è stato, inizialmente, tracciato, dalla L. del 15 marzo 1997, n. 59 (Gu n. 63 del 17 marzo 1997, So 57/L), che all'art. 15, comma 2, stabilisce che "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*".
A seguito della L. 59/1997, sono stati emanati il DPR del 10 novembre 1997, n. 513 (Gu n. 60 del 13 marzo 1998), recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici; il DPCM del 8 febbraio 1999 (Gu n. 87 del 15 aprile 1999), recante regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale dei documenti informatici, il DPR del 28 dicembre 2000, n. 445 (Gu n. 42 del 24 febbraio 2000, So 30/L), testo unico delle disposizioni legislative e regolamentari in materia di documentazione, successivamente modificato dal D.Lgs. del 23 gennaio 2002, n. 10 (Gu n. 38 del 15 febbraio 2002) (1); il DPR del 7 aprile 2003, n. 137 (Gu n. 138 del 17 giugno 2003), recante disposizioni di coordinamento in materia di firme elettroniche; ed infine, il D.Lgs. del 7 marzo 2005, n. 82 (Gu n. 112 del 16 maggio 2005, So 93), recante codice dell'amministrazione digitale, modificato dal D.Lgs. del 4 aprile 2006, n. 159 (Gu n. 99 del 29 aprile 2006, So 105).
Il codice dell'amministrazione digitale ha affrontato, per la prima volta, in modo organico e sistematico, le problematiche inerenti all'applicazione

dei fondamentali principi giuridici ai processi di digitalizzazione della PA.
Il documento informatico è, secondo la definizione data dal DPR 513/97, e, da allora, rimasta inalterata, "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".
La firma digitale, invece, è definita, dall'art. 1 del codice dell'amministrazione digitale come "*un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare, tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità del documento informatico o di un insieme di documenti informatici*".
La chiave privata, nel sistema di firma digitale, è conosciuta dal solo soggetto titolare e l'algoritmo che la genera è contenuto in un dispositivo di *smartcard*. (2) I dispositivi e le procedure utilizzate per la generazione delle firme, oltre ad essere sicuri, devono garantire l'integrità dei documenti informatici cui la firma si riferisce. La corrispondente chiave pubblica consente la verifica della sottoscrizione apposta al documento informatico dal titolare della firma.
Affinché possa essere garantita la corrispondenza biunivoca tra la chiave pubblica e il soggetto titolare cui essa appartiene, occorre che il certificatore rilasci un certificato elettronico qualificato, cioè un attestato elettronico che collega i dati, utilizzati per verificare le firme elettroniche, ai titolari.
L'art. 20, comma 2, D.Lgs. 82/2005, stabilisce che il documento informatico, sottoscritto con firma digitale "*formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile*".
Secondo l'art. 21, comma 2, il documento informatico, sottoscritto con firma digitale ha l'efficacia probatoria prevista dall'art. 2702 cod. civ. e l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria. Quindi, in questo caso, il documento fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi lo ha sottoscritto.(3)

3. - Nella prospettiva del DPR 123/2001 è ammessa la formazione, la comunicazione e la notificazione di atti del processo civile mediante documenti informatici; la trasmissione, comunicazione o notificazione dei documenti informatici sono effettuate per via telematica attraverso il sistema informatico civile (art. 2, commi 1 e 2). (4)
La struttura del sistema informatico civile consente di: individuare l'ufficio giudiziario e il procedimento, individuare il soggetto che inserisce, modifica o comunica l'atto, assicurare l'avvenuta ricezione della comunicazione dell'atto, nonché l'automatica abilitazione del difensore e dell'ufficiale giudiziario (art. 3, comma 1, DPR 123/2001).
Il DM del 14 ottobre 2004 ha indicato, specificamente, i soggetti abilitati ad accedere al sistema informatico civile. In linea generale, sono definiti soggetti abilitati tutti coloro ai quali è consentito fruire dei servizi di consultazione delle informazioni e trasmissione di documenti informatici relativi al processo. Prosegue, poi, l'art. 2, lett. i), DM 14 ottobre 2004, distinguendo i soggetti abilitati in interni ed esterni, e, tra quelli esterni, i soggetti privati e pubblici. Soggetti interni sono i magistrati, il personale degli uffici giudiziari e dell'UNEP (ufficio notifiche, esecuzioni e protesti); soggetti esterni pubblici sono gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali; soggetti esterni privati sono, infine, i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice.
Al fine di rendere possibile il compimento delle operazioni processuali informatizzate, descritte dal DPR 123/2001, il decreto ministeriale regolamenta il funzionamento delle strutture tecniche di cui si compone e secondo cui è organizzato il sistema informatico civile mediante le quali vengono gestiti i flussi informatici.
Il gestore centrale è l'unico punto di interazione, a livello nazionale, tra il sistema informatico civile e i soggetti abilitati esterni, attivo presso il Ministero della Giustizia, ed è definito come la "*struttura tecnico-*

organizzativa che, nell'ambito del dominio giustizia, […], fornisce l'accesso al sistema informatico civile ed i servizi di trasmissione telematica dei documenti informatici processuali" tra questo e i soggetti abilitati (art. 2, lett. b).

Il punto di accesso, a sua volta, è la struttura che "*fornisce ai soggetti abilitati, esterni al sistema informatico civile, i servizi di connessione al gestore centrale e di trasmissione telematica dei documenti informatici relativi al processo, nonché la casella di posta elettronica certificata*" (art. 2, lett. e). Il punto di accesso può essere attivato e gestito, secondo il dettato dell'art. 6, DM del 14 ottobre 2004, esclusivamente dai consigli dell'ordine degli avvocati, limitatamente ai propri iscritti; dal Consiglio Nazionale Forense, limitatamente ai propri iscritti e agli iscritti dei consigli dell'ordine degli avvocati; dal Consiglio Nazionale del Notariato, limitatamente ai propri iscritti; dall'Avvocatura dello Stato, dalle amministrazioni statali o equiparate e dagli enti pubblici, limitatamente ai propri iscritti e dipendenti; dal Ministero della Giustizia, ma solo per i soggetti abilitati interni ed in via residuale. Il punto di accesso può anche essere attivato e gestito da soggetti privati, purché, però, questi abbiano forma di società per azioni e rispondano ai requisiti di onorabilità previsti dall'art. 25, comma 1, del D.Lgs. del 1 settembre 1993, n. 385.

I soggetti abilitati esterni, quindi, accedono al sistema informatico civile, tramite un punto di accesso, ossia il servizio di interfacciamento del dominio giustizia, che, connette i soggetti stessi direttamente al gestore centrale.

Per consentire l'accesso al sistema informatico civile è necessario procedere, previamente, alla autenticazione dei soggetti abilitati, cioè alla loro identificazione in rete che avviene secondo le specifiche previste dalla carta nazionale dei servizi (art. 30, DM 14 ottobre 2004).

Le connessioni tra i punti di accesso e il gestore centrale, quindi le comunicazioni con l'esterno del dominio giustizia, avvengono mediante collegamento diretto alla Rete Unitaria della Pubblica Amministrazione (RUPA). (5)

Diversamente, i soggetti abilitati interni accedono al SIC tramite la Rete unica della Giustizia (RUG) e tramite il punto di accesso del Ministero della Giustizia.

Il gestore locale, invece, è il "*sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o all'UNEP, ed i servizi di trasmissione telematica dei documenti informatici processuali tra il gestore centrale ed il singolo ufficio giudiziario o UNEP*" (art. 2, lett. c). Il gestore locale fornisce servizio di consultazione del sistema informatico dell'ufficio giudiziario, per i soggetti abilitati esterni, collegati attraverso il gestore centrale, nei limiti dei privilegi di accesso dell'utente (art. 22, commi 1 e 2, DM 14 ottobre 2004). Inoltre, gestisce la trasmissione dei documenti tra i sistemi informatici dell'ufficio giudiziario o dell'UNEP ed il gestore centrale.

I l gestore centrale ed i gestori locali comunicano, tra loro, esclusivamente mediante la Rete Unica della Giustizia (RUG). La RUG è collegata alla RUPA e ciò consente "*le operazioni di trasporto, interoperabilità e cooperazione applicativa tra il sistema informativo giustizia ed i sistemi informativi di amministrazioni pubbliche diverse*"; inoltre, "*il collegamento alla RUPA consente nuovi sistemi di accesso ad informazioni, documentazione e servizi, e ciò sia per gli accessi dell'amministrazione della giustizia, sia viceversa per gli accessi agli archivi della stessa […]*". Infatti, il fatto di adottare il "*paradigma ipertestuale, analogo a quello su cui si basano i servers della rete Internet, consente di affiancare poi, alla disponibilità in linea dei documenti, la possibilità di interrogazioni semplici di archivi di documenti tra loro indipendenti, attraverso consultazioni ipertestuali contemporanee di più banche dati […], con il valore aggiunto che deriva dalla correlazione dei dati*". (6)

Tra le funzioni principali del gestore centrale rientrano, in particolare, quella di attestare temporalmente l'evento di ricezione dei documenti informatici che vi pervengono e quella di inoltrarli automaticamente verso il gestore locale e da questo verso l'esterno, alla casella di posta elettronica certificata dei soggetti abilitati.

4. - Le comunicazioni con biglietto di cancelleria e la notificazione dei documenti informatici del processo può avvenire, oltre che tramite sistema informatico civile, anche tramite posta elettronica (art. 6, DPR 123/2001).

L'indirizzo del difensore, tramite il quale avvengono le comunicazioni e le notificazioni, è unicamente quello che l'avvocato avrà comunicato al consiglio dell'ordine di appartenenza.
Un particolare tipo di posta elettronica disciplinata nell'ambito del processo telematico dal DM del 14 ottobre 2004 è la posta elettronica certificata. (7)
Il DM del 14 ottobre 2004 dispone che per utilizzare i servizi di trasmissione telematica dei documenti informatici, e quindi per poter inviare e ricevere dati e comunicazioni attinenti al processo e per effettuare notificazioni, occorre che i soggetti abilitati esterni dispongano di un indirizzo elettronico e della relativa casella di posta elettronica certificata, che vengono forniti dal punto di accesso. Ogni casella di posta elettronica certificata del processo telematico è abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale (art. 11, DM 14 ottobre 2004).
L'utilizzo della posta elettronica certificata consente, oltre alla conoscibilità certa della casella mittente e quindi del titolare, anche la possibilità di legare la trasmissione con il documento trasmesso.
Gli indirizzi elettronici e la relativa casella di posta elettronica certificata vengono attivati da ogni punto di accesso, su richiesta scritta di registrazione dell'interessato, il soggetto abilitato esterno, cui deve essere allegato certificato, rilasciato dal consiglio dell'ordine di appartenenza, attestante l'iscrizione all'albo. Lo stesso vale per gli esperti e gli ausiliari del giudice, che, al momento della registrazione, presentano il certificato di iscrizione all'albo dei consulenti tecnici o la copia della nomina del giudice, da cui deve risultare che l'incarico non sia esaurito.
Gli indirizzi e le informazioni sui richiedenti vengono conservati in un apposito registro che ogni punto di accesso deve attivare, in cui sono contenuti, oltre agli indirizzi emessi, anche quelli revocati o sospesi (art. 16, DM 14 ottobre 2004).
I singoli registri attivati dai punti di accesso, e le informazioni in essi contenute, confluiscono nel registro generale degli indirizzi elettronici, attivo presso il gestore centrale (art. 13, DM 14 ottobre 2004). Le copie dei registri locali e di quello nazionale sono consultabili per via telematica, ai sensi degli artt. 18 e 19 del decreto ministeriale, garantiscono la veridicità delle informazioni contenute e sono, costantemente, aggiornate dal personale autorizzato; i registri originali, invece, rimangono inaccessibili dall'esterno.
L a casella di posta certificata, è definita, nell'Allegato B del DM in esame, come una "*casella di posta elettronica alla quale è associata una funzione che rilascia delle ricevute di avvenuta consegna al ricevimento di messaggi di posta certificata*".
La necessità di assicurare la sicurezza degli scambi di comunicazioni impone un sistema di verifica e controllo dei messaggi inviati. Le operazioni di verifica sono effettuate dal gestore centrale, mentre il punto di accesso ha il compito di mantenere in linea i documenti informatici inviati fino a quando non riceve avviso di consegna dal gestore centrale o dal punto di accesso del destinatario.
Al momento dell'invio di un messaggio di posta certificata, il sistema verifica, preliminarmente, l'identità del mittente e dei dati di certificazione, che descrivono il messaggio originale; è necessario, poi, controllare che il messaggio non contenga *virus* informatici e che sia formalmente valido e privo di anomalie.
Una volta che siano stati compiuti i controlli necessari ed il messaggio risulti validamente formato, il mittente riceve, nella sua casella di posta, una ricevuta di accettazione, cioè a dire che il sistema ha accettato il messaggio. L'accettazione garantisce la correttezza formale del messaggio originale.
S e , invece, il messaggio contiene degli errori o è privo dei dati necessari per essere instradato nella casella di posta del destinatario, il mittente riceverà un messaggio di errore contenente l'avviso del rifiuto del messaggio e l'indicazione degli elementi mancanti.
I l documento informatico, inviato dal soggetto abilitato esterno, è ricevuto dal sistema informatico civile nel momento in cui il gestore centrale lo accetta ed attesta il momento temporale della ricezione. Contestualmente, il gestore centrale fornisce un servizio di inoltro automatico, previo controllo, di tutti i documenti informatici ricevuti dall'interno del sistema informatico civile verso l'indirizzo elettronico di destinazione.
La ricezione effettiva dal destinatario del messaggio viene attestata con

una ricevuta di avvenuta consegna, nel momento in cui il messaggio stesso è inserito nella casella di posta certificata del destinatario.(8)
La casella di posta certificata permette, anche, di effettuare i servizi di notificazione degli atti processuali informatici che avviene secondo le modalità descritte dall'art. 45 del decreto ministeriale del 2004. Le richieste di notifica dei difensori pervengono all'UNEP mediante inoltro del documento dal punto di accesso del mittente, tramite intermediazione e controllo del gestore centrale. Le richieste di notifica che provengono, invece, dagli uffici giudiziari, sono inoltrate, tramite la RUG, verso il sistema informatico dell'UNEP.
A d avvenuta notificazione dell'atto, il sistema informatico dell'UNEP invia, a chi ha richiesto il servizio, il documento informatico corredato di relata di notifica, costituita dalla ricevuta elettronica, sottoscritta dall'ufficiale giudiziario con firma digitale.
L e notifiche tra difensori consistono, invece, in uno scambio di messaggi tramite le rispettive caselle di posta certificata, mediato dal gestore centrale che provvedere a corredare i messaggi e le ricevute di avvenuta consegna delle necessarie attestazioni temporali.

5. - Gli artt. 9 ss. del DPR 123/01 disciplinano la costituzione in giudizio delle parti, il deposito degli atti e l'iscrizione a ruolo della causa, nonché la formazione del fascicolo informatico. Sia la procura alle liti sia la nota di iscrizione a ruolo possono essere trasmesse per via telematica e sottoscritte con firma digitale.
La parte che procede alla iscrizione a ruolo o alla costituzione in giudizio trasmette per via telematica i documenti probatori come documenti informatici o le copie informatiche dei documenti probatori su supporto cartaceo (art. 9).
Il difensore che si costituisce per via telematica trasmette la copia informatica della procura alle liti, nel caso in cui sia stata conferita su supporto cartaceo, e ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale (art. 10).
Anche la nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale (art. 11).
La cancelleria che riceve i documenti informatici del processo procede, con essi, alla formazione informatica del fascicolo d'ufficio e, contestualmente, anche alla formazione del medesimo fascicolo su supporto cartaceo. Nel fascicolo informatico sono inseriti anche i documenti probatori comunque acquisiti al processo (art. 12).
I fascicoli informatici ricevono la stessa numerazione dei fascicoli cartacei e l'indice informatico degli atti contiene, anche, l'indicazione dei documenti conservati solo nel fascicolo cartaceo; è, inoltre, redatto in modo tale da consentire la diretta consultazione degli atti e dei documenti informatici in esso elencati. Il fascicolo informatico contiene, altresì, apposite sezioni, ciascuna contenente l'indicazione del giudizio e della parte cui si riferiscono, nelle quali vengono inseriti gli atti e i documenti probatori depositati dalle parti, contestualmente alla costituzione in giudizio o successivamente. Il fascicolo informatico è consultabile dalla parte, oltre che per via telematica, anche nei locali della cancelleria attraverso un videoterminale (art. 13).
Ogni successivo atto del processo, documento probatorio e la sentenza del giudice vengono redatti come documenti informatici sottoscritti con firma digitale, trasmessi e depositati per via telematica. In particolare, il processo verbale d'udienza, redatto come documento informatico, viene sottoscritto con firma digitale dal giudice e dal cancelliere; nel caso in cui esso contenga le dichiarazioni rese dai testimoni o dalle parti in udienza sarà sottoscritto con la firma digitale di ciascuno. Se non è possibile procedere alla sottoscrizione digitale, il processo verbale viene redatto e stampato su supporto cartaceo, sottoscritto nei modi ordinari e allegato al fascicolo cartaceo. La copia informatica del processo verbale viene, però, comunque allegata al fascicolo informatico (art. 5, commi 1 e 2).
Il consulente tecnico d'ufficio trasmette la sua relazione, come documento informatico sottoscritto con firma digitale, e, con lo stesso mezzo, allega ad essa i documenti e le osservazioni delle parti, o la copia informatica di questi se sono stati prodotti su supporto cartaceo. Gli originali dei documenti, forniti dalle parti su supporto cartaceo, devono essere depositati dal consulente tecnico, prima della udienza successiva alla scadenza del termine per depositare le sua relazione (art. 15).

Dopo la precisazione delle conclusioni, il responsabile della cancelleria appone al fascicolo informatico la sua firma digitale.
La sentenza, redatta come documenti informatico e sottoscritta con firma digitale, viene trasmessa per via telematica al presidente del tribunale e al presidente della sezione di cui fa parte l'estensore, ed al cancelliere per il deposito. Ai fini del deposito, il cancelliere appone sulla sentenza la sua firma digitale.(9)
Il sistema di gestione del fascicolo informatico è, quindi, la parte del sistema dell'ufficio giudiziario dedicata all'archiviazione ed al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno dell'ufficio giudiziario. Oltre ai documenti informatici e agli allegati, sono inserite nel fascicolo informatico, anche, le ricevute brevi di avvenuta consegna e le attestazioni temporali degli scambi di messaggi intercorsi tra i soggetti abilitati esterni e gli uffici (art. 50, DM 14 ottobre 2004). I vari fascicoli informatici dei procedimenti giudiziari in corso sono conservati, per tutta la durata del procedimento, nell'archivio in linea dell'ufficio. Una volta conclusosi il procedimento i fascicoli vengono conservati presso gli uffici giudiziari competenti.
Il fascicolo informatico può essere trasmesso ai soggetti abilitati esterni, in tutto o in parte, e, in questo caso, il gestore locale provvederà a cifrarlo mediante un meccanismo di crittografia basato sulla chiave pubblica di cifratura del destinatario. Nel caso di richiesta di copia conforme del fascicolo, la conformità all'originale è attestata dal cancelliere e sottoscritta con la propria firma digitale.

6. - Dopo una lunga evoluzione normativa(10), nel 2000 è stato emanato il regolamento di disciplina della tenuta informatizzata dei registri di cancelleria con DM del 27 marzo n. 264 (Gu n. 225 del 26 settembre 2000).
Al regolamento ha fatto seguito il DM del 24 maggio 2001 (Gu n. 128 del 5 giugno 2001) che ha indicato, a norma degli artt. 1, comma 1, lett. f), e 3 del DM 264/2000, le regole procedurali relative ai registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero dei registri previsti da codici, leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dalla amministrazione della giustizia.
Oggetto del DM del 2001 è il sistema informativo, ossia "*l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione (sia in formato cartaceo, sia elettronico) che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti i registri informatizzati degli uffici*" (art. 1, comma 1).
Il sistema informativo è, dunque, l'intera struttura adibita alla gestione e alla utilizzazione dei registri informatizzati(11); esso deve essere organizzato in modo da garantire la disponibilità e l'integrità delle informazioni e dei servizi da parte degli utenti del sistema, l'autenticità dei dati, nonché il controllo degli accessi. Infatti, le informazioni possono essere fruite, e quindi create, modificate o cancellate, solo ed esclusivamente dalle persone autorizzate a compiere tali operazioni e secondo modalità predefinite (art. 2).
Responsabile della tenuta dei registri è il dirigente amministrativo dell'ufficio che è tenuto a produrre e mantenere aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informativo di sua competenza (art. 6).
È cura del responsabile della tenuta dei registri, con l'ausilio dell'amministratore del sistema, redigere il piano della sicurezza del sistema informativo (art. 3).
L'art. 7 del DM del 2001 indica le informazioni che il piano per la sicurezza deve contenere.
Oltre all'inventario delle risorse, devono esservi indicate le misure adottate per la protezione del sistema, in specie quelle per garantire la continuità degli applicativi relativi ai registri informatizzati in caso di malfunzionamento dei *server*, le misure adottate per la protezione fisica delle aree e dei locali interessati e quelle per la protezione dei dati e delle informazioni, nel rispetto anche delle norme in tema di trattamento dei dati personali.
Nel piano per la sicurezza devono, altresì, essere descritte le misure di monitoraggio del sistema, ossia le procedure di controllo e verifica della corretta esecuzione delle attività di utilizzo e gestione del sistema informativo, le modalità delle procedure di archiviazione ottica e di copia

storica dei dati e, infine, il piano di adeguamento degli applicativi.

7. - Per poter usufruire dei servizi offerti dalle strutture del processo telematico, i soggetti abilitati esterni devono avere delle postazioni di lavoro che gli consentano l'accesso al sistema informatico civile.
Il DM del 14 ottobre 2004, all'art. 36, descrive la postazione di lavoro come l'insieme delle risorse *hardware*, *software* e di rete utilizzate direttamente dai soggetti abilitati per la formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del sistema informatico civile.
La postazione di lavoro, inoltre, deve essere dotata delle risorse *hardware* e *software* necessarie alla gestione della firma digitale su *smartcard* e alla autenticazione per la connessione al punto di accesso.(12)
I soggetti del processo telematico dispongono, poi, di un certificato di crittografia necessario per la cifratura degli atti e, inversamente, per decifrare quelli crittati; allo stesso modo, gli uffici giudiziari automatizzati fruiscono della chiave e del certificato di cifratura con i quali possono cifrare gli atti depositati sul *client* dei soggetti abilitati.
Quindi, gli atti e i documenti redatti dai soggetti abilitati esterni, dalla postazione di lavoro, devono essere firmati e crittati per l'ufficio giudiziario di destinazione. Il gestore locale decifra i documenti crittografati che riceve e provvede a cifrare i documenti in uscita dai singoli uffici giudiziari o dall'UNEP. Inoltre, il gestore locale verifica automaticamente la firma digitale, apposta sul documento, e l'autenticità e l'integrità dei documenti informatici ricevuti. Controlla, a sua volta, il rispetto dei formati e l'assenza di *virus*, e, successivamente, rende disponibili i documenti ricevuti al sistema informatico di gestione delle cancellerie o dell'UNEP, associandovi le informazioni dell'attività di verifica, per valutarne la ricevibilità (art. 22, DM 14 ottobre 2004).
Il sistema informatico di gestione dell'UNEP funziona nel modo su descritto, acquisendo i documenti da notificare e restituendoli, completi di relata di notifica, a notificazione eseguita.
Il sistema informatico di gestione delle cancellerie, invece, cura l'accettazione del documento ricevuto aggiornando i registri ed il fascicolo informatico.
Quando il difensore invia all'ufficio giudiziario del ruolo generale del tribunale un atto per la iscrizione della causa a ruolo, il sistema informatico di gestione comunica, per via telematica, una comunicazione recante il numero di ruolo del procedimento assegnato dall'ufficio competente a conoscere la causa.

8. - Come si può osservare dalla lettura delle norme sul processo telematico e le relative regole tecniche, non si assiste ad alcuna modificazione delle procedure giudiziarie, ma soltanto alla automazione delle fasi processuali.(13) Il progetto di automazione del processo ha trovato avvio, in via sperimentale, in alcuni tribunali italiani tra cui quelli di Bari, Lamezia Terme, Bergamo, Bologna, Catania, Genova e Padova.
In particolare, il gruppo di lavoro di Bologna ha messo a punto, dal 1993, un progetto denominato 'Polis', nell'ambito del quale è stato realizzato il primo sistema informativo per la produzione, archiviazione e consultazione delle decisioni, che consiste nella memorizzazione informatica del testo integrale di tutte le sentenze emesse dal Tribunale di Bologna, consultabili per via telematica da magistrati e avvocati.
La sperimentazione ha avuto avvio, informatizzando completamente le procedure d'urgenza relative ai ricorsi per ingiunzioni di pagamento e decreti ingiuntivi.
E dopo la fase di sperimentazione, di recente, il Tribunale di Milano ha avviato la fase operativa del processo civile telematico.
Inoltre, nel corso del 2004 sono state collaudate, nell'ambito del progetto di automazione, la consultazione a distanza dei registri di cancelleria e degli archivi dei documenti e la automazione delle attività di cancelleria e del giudice delle esecuzioni mobiliari e immobiliari. (14)
Ulteriormente, per quanto riguarda la realizzazione di servizi *on line* sono stati collaudati: il portale di accesso agli uffici giudiziari, il sistema per la pubblicità telematica delle aste giudiziarie il progetto *Norme in rete*, punto di accesso alla documentazione normativa pubblicata dalle amministrazioni pubbliche sul *web*, dal quale è possibile anche l'accesso al patrimonio normativo del CED della Corte Suprema di Cassazione.(15)
Una serie di iniziative sono state intraprese anche relativamente ai

sistemi informatici dell'area penale e della giustizia amministrativa.(16)

Note

(1) Il D.Lgs. 10/2002, emanato in attuazione della Direttiva europea 1999/93/CE (Guce n. L 13 del 19 gennaio 2000), relativa ad un quadro comunitario per le firme elettroniche, è stato abrogato dalla data di entrata in vigore del codice dell'amministrazione digitale.

(2) Cfr., l'art. 1, Titolo I, dell'allegato tecnico del DPCM del 8 febbraio 1999.

(3) Per una disamina delle diverse tipologie di firme elettroniche e della diversa validità ed efficacia probatoria del documento informatico, a seconda che sia sottoscritto con firma elettronica semplice, con firma elettronica qualificata o con firma digitale, si rinvia a W. D'Avanzo, *L'e-government*, Movimedia, Lecce, 2007, pp. 33-34 e pp. 45 ss.

(4) La previsione della trasmissione dei documenti informatici per via telematica segue l'orientamento costante del legislatore, il quale, fin dal 1993, ha previsto modalità alternative ai tradizionali mezzi di trasmissione dei documenti cartacei. Secondo il dettato della L. del 7 giugno 1993, n. 183 (Gu n. 137 del 14 giugno 1993), gli avvocati possono trasmettere copia di documento processuale ad altro avvocato tramite telefax. Il DPR 513/1997 ha, poi, disciplinato le modalità di trasmissione, per via telematica, del documento informatico, che si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. Il D.Lgs. del 17 gennaio 2003, n. 5 (Gu n. 17 del 22 gennaio 2003, So 8), sul nuovo rito societario, prevede la possibilità, per le parti costituite, di effettuare tutte le comunicazioni e notificazioni a mezzo fax o per posta elettronica. Cfr. F. Mirabelli, *Il processo civile telematico*, in G. Riem, A. Sirotti Gaudenzi, *La giustizia telematica e la procedura informatizzata*, Maggioli, Rimini, 2005, p. 54.

(5) Le Rete Unitaria della Pubblica Amministrazione (RUPA) è stata istituita dell'art. 5, comma 1, della L. 59/1997e può essere definita come l'insieme dei domini, ciascuno inteso come l'insieme delle risorse *hardware*, di comunicazione e di *software* di competenza di una determinata amministrazione, organizzato in un interdominio centrale, costituito da una dorsale, cioè da un sistema di *routers* o nodi, "*in grado di instradare i vari messaggi, e dotato di tante porte di rete quanti sono i domini delle amministrazioni connesse*"; v., F. Buffa, *Il processo civile telematico. La giustizia informatizzata*, Giuffrè, Milano, 2002, p. 40. Scopo della RUPA è quello di garantire a qualunque utente della rete, purché autorizzato e in condizioni di sicurezza, "*di poter accedere ai dati e alle procedure dei sistemi informativi automatizzati della propria e delle altre amministrazioni, indipendentemente dalle reti attraversate e dalle tecnologie utilizzate dai singoli sistemi informativi*"; sul punto, M. Iaselli, *La rete unitaria della P.A.*, in G. Cassano (a cura di), *Diritto delle nuove tecnologie informatiche e dell'Internet*, Ipsoa, Milano, 2002, p. 1278. I livelli applicati della RUPA sono stati ridefiniti dal D.Lgs. del 28 febbraio 2005, n. 42 (Gu n. 73 del 20 marzo 2005), che ha istituito il Sistema Pubblico di Connettività (SPC) e la Rete Internazionale della Pubblica Amministrazione (RIPA). Questo decreto è confluito nel codice dell'amministrazione digitale a seguito della modifica al codice intervenuta con il D.Lgs. 159/2006 che ha previsto, peraltro, un termine per la cessazione dell'operatività della RUPA e la sua sostituzione con il SPC.

(6) F. Buffa, cit., pp. 46-47.

(7) A partire dal riferimento primario costituito dall'articolo 15, comma 2, della L. 15 marzo 1997, n. 59, il quadro normativo di riferimento relativo alla posta elettronica certificata è costituito dal DPR del 11 febbraio 2005, n. 68 (Gu n. 97 del 28 aprile 2005), regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della L. del 16 gennaio 2003, n. 3; dal DM del 2 novembre 2005 (Gu n. 265 del 14 novembre 2005), recante le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata; dalla Circolare CNIPA CR/49 del 24 novembre 2005 (Gu n. 283 del 5 dicembre 2005), che ha disciplinato le modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata; dal codice dell'amministrazione digitale.

(8) Si veda l'Allegato B del DM del 14 ottobre 2004.

(9) Per quanto riguarda le sentenze, particolare importanza rivestono le

procedure informatiche di redazione degli atti, con notevoli vantaggi specie per quanto riguarda la semplificazione dell'attività giurisdizionale. I sistemi esperti, la giurimetrica, il deposito e la trasmissione della sentenza costituiscono una evoluzione delle tecnologie a servizio dell'amministrazione della giustizia. Per una completa disamina della sentenza telematica, si veda F. Buffa, cit., pp. 143-162.

(10) Sul punto, v., *ivi*, pp. 177 ss.

(11) P . Vincenzotto, *La riservatezza e la sicurezza del sistema informativo negli uffici giudiziari*, in G. Riem, A. Sirotti Gaudenzi, cit., p. 138.

(12) L'avvocato può scegliere il proprio sistema informatico e il suo *Internet service provider* che gli assicuri la connessione al dominio giustizia. In particolare, gli avvocati utilizzano ambienti *software* integrali che consentono le funzionalità di gestione dello studio legale e la comunicazione interattiva con altri ambienti con piena integrazione tra i vari momenti dell'attività legale. Inoltre, l'avvocato connesso *on line* può operare direttamente presso gli uffici giudiziari; v. F. Buffa, cit., pp. 199 ss.

(13) M. Cammarata, *"Tutti gli atti e i provvedimenti del processo..."*, in *Interlex* (www.interlex.it).

(14) Si veda il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2005-2007, a cura del CNIPA, in www.cnipa.gov.it.

(15) Si veda il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2006-2008, a cura del CNIPA, in www.cnipa.gov.it.

(16) Le iniziative hanno come obiettivo, in ambito penale, migliorare l'efficienza del sistema penale nelle varie fasi processuali, dalla attività investigativa fino al momento della esecuzione penale. I principali progetti correlati alla automazione della fase investigativa riguardano la riorganizzazione dei centri per le intercettazioni telefoniche, finalizzata alla costituzione di un sistema unitario che preveda la registrazione e la gestione computerizzata dell'archiviazione; il progetto EPOC (*European Pool against Organized Crimes*) per il supporto alla raccolta, analisi, uso e scambio di informazioni di interesse per le indagini di criminalità organizzata eseguite in paesi diversi e presso diversi uffici investigativi. L'automazione del processo penale prevede, poi, la riorganizzazione del Sistema Integrato Esecuzione e Sorveglianza (SIES), per la condivisione del patrimonio informativo degli uffici giudiziari e la gestione documentale e archiviazione delle sentenze. Ulteriori azioni sono correlate alla automazione ed integrazione delle banche dati e dei flussi informativi strumentali alle azioni di contrasto alla criminalità organizzata, tra cui, ad esempio, l'acquisizione telematica delle notizie di reato e la comunicazione elettronica delle notizie di reato; la realizzazione del sistema per la gestione delle misure cautelari personali, per consentire il monitoraggio dei termini di scadenza e prevenire il rischio di scarcerazioni. I nuovi progetti riguardano il Sistema informativo dibattimentale, per la gestione multimediale del dibattimento attraverso la realizzazione di un sistema di archiviazione digitale multimediale, sincronizzazione e *information retrieval* degli atti del dibattimento penale, e la realizzazione del Sistema Integrato dell'Area Penale (SIAP), per la condivisione del patrimonio informativo digitale delle procure e la piena integrazione con i sistemi di casellario, della Cassazione e dell'amministrazione penitenziaria. Per quanto riguarda l'ambito della giustizia amministrativa, il cittadino, che ne abbia interesse, e le parti, gli avvocati e le amministrazioni centrali e locali, possono consultare sul sito dell'amministrazione lo *status* dei ricorsi dal deposito iniziale fino alla emissione del provvedimento. È consentito, inoltre, consultare i provvedimenti emessi sui singoli ricorsi a partire dall'ottobre del 2000. Vengono infine rese disponibili informazioni sulla normativa e sul funzionamento del processo amministrativo. Le iniziative e i progetti su menzionati sono descritti nei Piani triennali per l'informatica nella PA, 2005-2007 e 2006-2008, cit., curati dal CNIPA.