PROCEDURE ET IMMATERIEL

RAPPORT NATIONAL TURQUIE

Ebru Ay Chelli

Docteur en droit
Maître de conférences
Université d'Économie d'Izmir

L'efficacité et la célérité de la justice constituent des préoccupations majeurs au regard des différentes politiques menées ces dernières années. La lenteur de la justice fait partie des plus importantes critiques adressées à l'institution. Or, la constante augmentation du nombre des requêtes et plaintes déposées devant les tribunaux n'est pas sans conséquence sur les délais de traitement des affaires. Ainsi pour l'année 2013, 895.392 affaires ont été déposées devant la Cour de cassation turque (JO du 29 janvier 2014).

Face à ce constat et à la nécessité d'un meilleur « rendement » de la justice, l'utilisation des nouvelles technologies se doit d'engendrer un gain de temps, une diminution des déplacements, une accélération de la transmission des informations et une meilleure gestion des affaires au bénéfice du des usagers du service public de la justice, en l'occurrence les justiciables.

I – La cyberjustice ou UYAP

En droit turc, le terme cyberjustice n'est pas employé. C'est le Système Informatique Judiciaire National, *UYAP* qui intègre la cyberjustice qui est communément employé pour désigner cette notion. Il s'agit d'un système d'information centralisé qui dessert tous les tribunaux ainsi que l'ensemble des instances judiciaires, les prisons y comprises. Ce système d'information a été mis en place en 2000 par le Ministère de la Justice sur la base de l'article 141 de la Constitution disposant qu'« il incombe aux autorités judiciaires de régler les procès à moindres frais et dans les meilleurs délais ». *UYAP* est aujourd'hui un système mature, utilisé par la totalité des instances judiciaires en Turquie.

UYAP a été conçu et réalisé par le Département des Technologies de l'Information du Ministère de la Justice dans l'objectif de procurer des services en ligne aux avocats et aux citoyens dans le cadre du projet e-gouvernement. Il s'agit d'un système qui permet l'intégration des bases du Ministère de la Justice et des autres agences et autorités affiliées à ce Ministère (prisons et autres établissements pénitentiaires), des bases de divers cours et tribunaux (Cour constitutionnel, Conseil d'État, Cour de Cassation, tribunaux de première instance et cours d'appel), ainsi que des bases d'autres institutions, comme les différents Ministères, les départements de police, le cadastre, le service des

statistiques, les organismes de sécurité sociale, divers établissements publics etc. Cette intégration permet aux instances judiciaires d'avoir accès à un large éventail des données, dont la collecte devient nécessaire dans les procédures du contentieux civil, pénal ou administratif : par exemple, le juge peut avoir directement et immédiatement accès aux certificats de naissance et autres informations concernant l'état civil des justiciables ou aux registre des condamnations pénales.

UYAP offre les services suivants :

(a) Une banque de données électronique (Databank) qui permet à tout intéressé d'avoir accès à la législation, aux arrêts des tribunaux et par conséquent à la jurisprudence, à des articles et commentaires juridiques, à un lexique des termes juridiques.

(b) Le système d'information SMS :

L'inscription à ce système est immédiate et gratuite ; elle est effectuée par l'envoi de son numéro de carte d'identité personnel. Les notifications envoyées par le système ont elles un coût qui s'élève à une livre turque par notification ; ce système permet aux intéressés de recevoir immédiatement par SMS toutes informations et mises à jour concernant le litige, sans nécessité de se déplacer au greffe du tribunal compétent.

(c) Un service électronique pour la formation continue des juges, des procureurs et du personnel administratif des instances judiciaires, notamment s'ils désirent recevoir un traitement sur les modalités et les techniques d'utilisation de l'UYAP.

(d) Un webmail qui permet aux usagers intéressés d'avoir accès à un compte e-mail pour partager des informations.

(e) Un forum de discussion où les usagers peuvent aussi discuter des questions juridiques et partager leurs idées et expériences.

(f) Un portal pour les citoyens qui peuvent avoir accès au système avec leur signature électronique et effectuer certaines démarches procédurales dans les affaires les concernant.

(g) Un portal pour les avocats qui, en fonction de leur autorisation, peuvent avoir accès aux dossiers des litiges où ils sont parties, imprimer des documents, ajouter des documents à un dossier, déposer une requête, faire les paiements nécessaires etc ; si certaines conditions sont réunies et toujours sur autorisation du juge, les avocats peuvent aussi avoir accès aux documents des dossiers où ils ne sont pas parties.

(h) Un portal spécial pour les personnes morales du secteur public.

(i) Un portal pour les experts qui peuvent examiner les dossiers nécessitant une expertise, rédiger leurs rapports et les soumettre après les avoir approuvés par signature électronique.

Le principal objectif visé dans UYAP est l'accélération et la simplification des opérations, la création d'un système d'information fiable, transparent et efficace, qui permet aux justiciables d'avoir accès aux informations les concernant à tout moment et sans se déplacer, la réduction des coûts et de la bureaucratie.

De plus, après la fin d'une phase de test, les tribunaux et autres instances judiciaires sont équipés de l'enregistrement audiovisuel, d'un système de conférence vidéos et d'un système de transcription électronique. Les règles régissant le fonctionnement du système, nommé SEGBIS, est prévu dans le règlement du 20 septembre 2011 quant à la procédure pénale et dans celui du 3 avril 2012 quant à la procédure civile. Par exemple selon l'article 60 de ce dernier, le juge ou le tribunal peut, avec le consentement des parties, leur permettre de participer à l'audience et d'accomplir des actes de procédure à distance. Sous réserve du consentement des parties, le juge ou le tribunal peuvent permettre aux témoins, aux experts ou aux parties d'être entendus à distance via SEGBIS. Ceci est également valable pour les prestations de serment des parties.

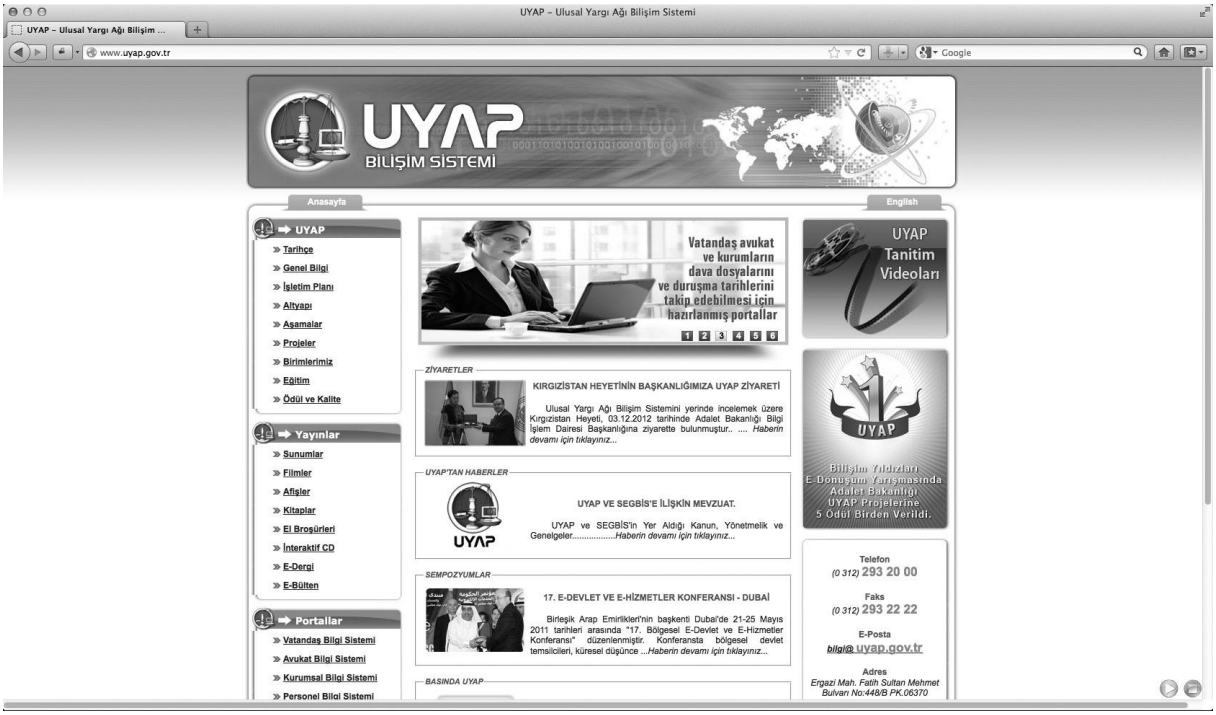
Les personnes présentes à l'enregistrement, doivent apposer leur signature manuscrite sur le procès-verbal ou signer numériquement sur UYAP que les identités des intéressés ont été dûment contrôlées et que l'audio conférence a été menée à bien. Dans le procès-verbal figurent les noms et prénoms des personnes entendues, les heures de début et de fin de l'enregistrement, la durée de celui-ci, les personnes présentes à l'enregistrement ainsi que les preuves avancées.

Pour pouvoir utiliser ce système, les tribunaux doivent être dotés des équipements suivants : Caméra IP, microphone, mixeur audio, moniteur audio, système d'archivage de données, logiciel de vidéo-conférence, dictée vocale et casque.

Actuellement, un peu plus de 3000 installations ont été réalisées et ces systèmes continuent à être déployés dans le pays.

Enfin, dans le cadre du processus d'adhésion à l'Union Européenne, un rapprochement des données contenues dans UYAP avec d'autres bases de données centrales de l'UE et les systèmes des pays membres est envisagé.

Le système UYAP est en effet remarquable et a déjà reçu en 2008 le prix « Balance de cristal» pour des pratiques innovantes concourant à la qualité de la justice civile.



Site web d'UYAP

II – L'encadrement des technologies de l'information et des communications

Les technologies de l'information et des communications sont encadrées par plusieurs lois et de règlements.

Ces législations sont citées ci-dessous par ordre chronologique :

- Loi sur la signature électronique n° 5070 du 23 janvier 2004

La loi du 23 janvier 2004 relative à la signature électronique définit dans son article 3 la « signature électronique » comme « des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, étant utilisées pour identifier le signataire dans le cadre du message de données ».

L'article 5 prévoit, par ailleurs, que « la signature électronique sécurisée est assimilée à la signature manuscrite». Cette disposition est reprise par l'article 14 du Code des obligations qui y ajoute un deuxième alinéa prévoyant que «celle qui procède de quelque moyen mécanique n'est tenue pour suffisante que dans les affaires où elle est admise par l'usage, notamment lorsqu'il s'agit de signer des papiers-valeurs émis en nombre considérable». Cependant la signature électronique n'est pas admise dans les hypothèses pour lesquelles l'acte authentique est exigé à titre de validité.

Selon l'article 4 de la loi sur la signature électronique, la signature électronique sécurisée est une signature qui :

a) n'est attribuée qu'au possesseur de la clef de chiffrement,

b) est créée par des moyens que le possesseur de la clef de chiffrement peut garder sous son contrôle exclusif,
c) permet d'identifier le possesseur de la clef de chiffrement,
d) est liée de telle manière aux données auxquelles elle se rapporte que toute modification ultérieure des données soit détectable.

La vérification de la signature électronique repose sur l'utilisation d'un certificat électronique qualifié qui permet de garantir l'identité du signataire. Selon l'article 9 de la loi, les certificats devront comprendre un certain nombre de mentions obligatoires telles que : l'identité du prestataire de service de certification qui délivre le certificat, le nom du signataire, la période de validité du certificat, ses conditions d'utilisation, etc...

En outre, l'article 10 de cette même loi pose un certain nombre de conditions se rapportant au prestataire de service de certification (ci-après PSC). Elles concernent notamment la fiabilité des services de certification, l'application de procédures de sécurité adaptées, la concordance des données de création et des données de vérification, la conservation des informations relatives au certificat.

Le règlement du 6 janvier 2005 décrit la procédure à suivre en vue de la reconnaissance de la qualification de PSC. Le droit turc ne détermine pas les modalités d'accréditation des organismes qui procèdent à l'évaluation des PSC car un tel système n'existe pas. Il n'y a donc pas de différence, en droit turc, entre une signature électronique certifiée et accréditée quant à leur force probante.

Ainsi et pour ne citer que quelques exemples parmi les prestataires les plus connus on trouvera : E Guven (www.e-guven.com), Governmental Certification Center (www.kamusm.gov.tr), TürkTrust (www.turktrust.com.tr), etc. Cette dernière compagnie, société de droit privé, fournit à l'Union des barreaux de Turquie une solution de signature électronique pour accéder au système UYAP. Les procédures entre les différentes branches du système judiciaire et les autres organismes officiels ont été totalement intégrées et automatisées sur l'infrastructure de signature électronique dans UYAP dématérialisant les échanges et s'affranchissant du document papier.

Les certificats sont proposés sur support logiciel, carte à puce ou clé USB.

- Loi n° 5651 du 4 mai 2007 sur « la réglementation des publications diffusées sur internet et visant à combattre les délits de presse via internet »

La loi de 2007 a pour objet de fixer les obligations des fournisseurs d'accès internet, des hébergeurs de sites web et des fournisseurs d'accès internet grand public et de combattre via ces fournisseurs certains délits commis sur internet.
La suppression de l'accès à internet n'est possible que sous le contrôle d'un juge. En effet, lorsque le parquet est saisi d'une plainte ou par suite de ses propres constatations, il peut demander à un juge d'ordonner l'interdiction d'accès au site web en question dans un délai de vingt-quatre heures. Le parquet peut, en cas d'urgence ordonner lui-même cette interdiction, qui doit ensuite être approuvée par un magistrat dans un délai de vingt-quatre heures. L'interdiction doit être appliquée dès que possible et exécutée par le fournisseur d'accès internet dans un délai de vingt-quatre heures à compter de l'ordonnance judiciaire.

En cas de rejet de l'interdiction par le juge, le parquet est tenu de rétablir intégralement l'accès au site web en question.
Il est intéressant de noter que ce blocage se fait via la simple modification des DNS des fournisseurs d'accès, mesure technique très rapide mais notoirement facile à contourner.

- Amendements du 5 février 2014 de la loi n° 5651 du 4 mai 2007

Les modifications apportées à la loi en février 2014 et notamment l'article 9, al. A, sur le « blocage de l'accès à internet en raison du respect de la vie privée » permettent à l'Autorité gouvernementale des télécommunications (*Telekomünikasyon İletişim Başkanlığı*, ci-après TIB) de bloquer sans décision de justice les sites internet portant atteinte à la « vie privée » ou publiant des contenus jugés « discriminatoires ou insultants » et autorisent la même TIB à requérir des informations sur les sites visités par chaque internaute auprès des fournisseurs d'accès et à les conserver pendant deux ans. Ces dispositions sont contraires à la Constitution turque en ses articles 13, 20, 22, 26 et à l'article 8 de la CEDH. Le législateur ne peut pas confier la possibilité de restriction de l'accès à Internet à une simple autorité administrative. En raison du principe constitutionnellement reconnu qu'est la liberté d'expression, seul un juge doit pouvoir interdire l'accès à Internet en raison de la gravité de l'atteinte à ce principe.

Il n'existe donc pas de contrôle a priori par le juge à l'heure actuelle, contrairement à la situation antérieure aux modifications de la loi du 4 mai 2007.

- Loi sur la communication électronique du 5 novembre 2008, n° 5809 :

Cette loi pose le cadre juridique général de la communication électronique codée et chiffrée et prévoit la rédaction ultérieure par la TIB d'un règlement de la procédure et des principes de communications codées et chiffrées.

- Le règlement relatif à la procédure et aux principes des communications électroniques codées ou chiffrées des institutions et organismes publiques et des personnes réelles et morales du 23 octobre 2010, JO n° 27738 :

Le règlement prévoit les modalités d'autorisation pour la production et l'import par les sociétés nationales et internationales des dispositifs de chiffrement ainsi que les modalités de communication moyennant l'usage ces dispositifs.

Selon l'article 5, al. 2, ç du Règlement, l'agrément de la TIB est accordé si les clés de chiffrement lui sont remises automatiquement par le producteur ou le vendeur de l'appareil de chiffrement. Si l'appareil a été acquis à l'étranger, l'utilisateur devra lui-même les remettre à la TIB. Ces clés seront gardées par la TIB (art. 8, al.2)

Le règlement imposant de livrer les clés de chiffrement à l'État, semblent en totale contradiction avec la Constitution et avec l'article 8 du CEDH prévoyant que « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Le règlement restreint sérieusement la notion de confidentialité inhérente à tout usage de chiffrement, celle-ci n'étant plus garantie dès lors que les clés ne sont plus confidentielles et ont été divulguées.

- Le règlement sur la signification et notification par voie électronique du 19 janvier 2013

Le règlement modifie la loi sur la notification de 1959 et y ajoute l'article 7/a, celui-ci disposant que :

“La signification et notification par voie électronique est faite par la transmission de l'acte à son destinataire, si ce dernier en fait la demande en produisant une adresse électronique valide. Elle est obligatoire pour les sociétés anonymes, les SARL et les sociétés en commandites par actions.
La signification et la notification par voie électronique est une signification réputée avoir été remise à l'adresse de son destinataire à la fin du 5ème jour qui suit la réception de l'acte. »

Les personnes morales indiquées à l'article 1 du Règlement doivent signifier ou notifier leur acte, en passant par la Poste, la seule instance compétente.

Ces personnes sont : Les administrations publiques, les administrations à compte d'affectation spéciale, les autorités de contrôle, les institutions de sécurité sociale, les administrations provinciales spéciales, les villages, les municipalités, les barreaux et les notaires.

Lesdites instances doivent également avoir une adresse de courrier électronique certifiée par la Poste, comme d'ailleurs les destinataires choisissant la signification par voie dématérialisée. Ces derniers peuvent obtenir une adresse certifiée par les prestataires de services avec leur signature électronique certifiée.

Les prestataires de service qui sont habilitées à fournir des adresses électroniques certifiées sont désignées par la TIB. Aujourd’hui les prestataires agréés sont trois sociétés anonymes : La poste (www.ptt.gov.tr), TNB (www.tnbkep.com.tr), TURKKEP (www.turkkep.com.tr).

L'acte à notifier ou à signifier est envoyé au destinataire par la Poste ou par le prestataire de service via la Poste. Le destinataire accède à son compte de notification électronique par sa clé ou par ses identifiants et mot de passe. C'est au prestataire de service de vérifier l'identité du destinataire.

III – Règles relatives à la preuve électronique

En droit turc, les règles de preuves électroniques sont prévues aux articles 205, al. 2 et 205, al. 3 du Code de procédure civile. Selon ces dispositions, « la force probante du document signé par voie électronique est équivalente à celle de l'acte sous seing privé ». Toutefois « le juge vérifie d'office la présence d'une signature électronique certifiée sur le document ». L'article 201 dispose d'autre part que si l'une des parties conteste l'existence d'un tel document, le juge, après avoir écouté cette partie, peut demander une expertise.

La dématérialisation des procédures vise à entraîner une diminution des coûtsengendrés par les dossiers papiers et à rendre le système de justice plus proche, plus simple et plus accessible tant aux justiciables et qu'aux opérateurs économiques.

Comme cela est le cas pour les récentes réformes en matière de procédure civile en Turquie, elle se fonde sur l'existence d'un principe de célérité qui fait l'unanimité dans un système qui se veut toujours plus performant et concurrentiel. Pourtant, la célérité ne doit pas fasciner au point d'aboutir à une perturbation de l'équilibre des pouvoirs au sein du procès ou à un affaiblissement des garanties de procès équitable. La célérité et la qualité du rendu de la justice sont des axes majeurs au sein d'UYAP.

La dématérialisation, plus qu'un simple changement de support à l'identique, induit un véritable changement de paradigme. L'adoption des technologies de l'information, outre l'aspect strictement technique, induit des besoins nouveaux sur le plan organisationnel pour assurer la sécurité, la disponibilité, l'intégrité et la tracabilité des données. Leur complexité intrinsèque les met hors de portée du contrôle des profanes si des procédures adéquates ne sont pas pensées et mises en place en amont. De plus, les systèmes d'information sont sujets à des disfonctionnements dont l'origine est parfois difficile à déterminer (logiciel, matériel, réseau...) et pouvant compromettre l'intégrité et la disponibilité des données. Ces aléas viennent s'ajouter aux erreurs, négligences voire aux malveillances humaines déjà existantes dans le système papier. En effet, les fraudes de l'ancien système trouvent leur équivalent dans leur homologue numérique, l'usurpation d'identité classique se retrouve dans le système dématérialisé. C'est ainsi que la peine d'emprisonnement de cinq ans d'un détenu a été modifiée, en utilisant la signature numérique du procureur, de manière à apparaître comme déjà effectuée dans le système d'UYAP. Ceci dit l'audit du système de journalisation informatique a permis de détecter la fraude. Les technologies de l'information, munies des procédures adéquates, et accompagnées d'une formation rigoureuse des utilisateurs et acteurs du système, peuvent donc présenter des avantages indéniables et même des garanties supérieures de sécurité, apportées par les outils cryptographiques modernes, par rapport au support papier.