Le Centre d'études juridiques et politiques de l'Université de La Rochelle (CEJEP/ EA 3170), dans le cadre de la recherche SHADES financée par l'Agence Nationale de la Recherche (ANR), propose, à compter du 1er septembre 2015, un contrat doctoral d'une durée de 3 ans sur la thématique suivante :

Dématérialisation et droit de la preuve

La mise au point d'un procédé visant à la création d'une signature qui serait propre à un document dématérialisé et qui permettrait avec certitude de l'authentifier soulève, en droit, un double questionnement : d'une part, quant au positionnement juridique de cette technique au regard des textes sur le droit de la preuve, la signature et l'archivage électroniques ; d'autre part, quant à l'intérêt qu'elle pourrait présenter pour les usagers, les justiciables et les praticiens du droit.

Après l'adoption de la directive 1999/93/CE du 13 décembre 1999 sur les signatures électroniques, la France s'est dotée d'une législation sur la preuve électronique avec la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. L'objectif était d'adapter les normes à la dématérialisation des supports, et, dans le même temps, de conserver l'unité des règles de preuves, afin d'éviter toute opposition entre la nouveauté et la tradition et d'assurer la confiance et la sécurité juridique. Les règles du Code civil relatives à la preuve ont été modifiées et des décrets d'application sont venus compléter le dispositif. Il en résulte que les grandes orientations du droit français peuvent se résumer ainsi : le champ d'admission de la preuve électronique a été élargi en rendant la preuve littérale indépendante de son support, ce qui a conduit à une équivalence juridique entre la preuve littérale électronique et la preuve traditionnelle sur support papier ; la signature électronique a été placée, à certaines conditions, au même rang que la signature manuscrite, ce qui permet de valider l'écrit sous forme électronique par l'apposition d'une signature électronique ; mais encore, ont été consacrés, d'une part, le caractère supplétif des règles de preuve et, d'autre part, le pouvoir du juge de trancher les conflits de preuve.

Selon le Code civil, la signature électronique consiste « en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans les conditions fixées par décret en Conseil d'État » (C. civ., art. 1316-4, al. 2). Ces conditions ont été posées par le décret n° 2001-272 du 30 mars 2001. Elles sont au nombre de trois : l'usage d'une signature électronique sécurisée, l'utilisation d'un dispositif sécurisé de création de signature électronique et l'utilisation d'un certificat électronique qualifié.

Il est à remarquer que la directive européenne de 1999, de laquelle dérive les textes français, opère une distinction entre « signature électronique » et « signature électronique avancée ». La première y est définie comme « une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ». La seconde est une signature électronique qui satisfait à quatre exigences: a) être liée uniquement au signataire; b) permettre d'identifier le signataire; c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Cette même directive définit le « signataire » comme toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou

personne physique ou morale qu'elle représente. Enfin, elle entend par « données afférentes à la création de signature », des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique.

Un pas supplémentaire a été franchi avec l'adoption du Règlement européen *eIDAS* (*electronic Identification and trust services for electronic transactions in the internal market*) du 23 juillet 2014 (Règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur). Ce texte privilégie deux axes :
- une reconnaissance mutuelle des moyens d'identification électronique entre tous les États membres ;
- la mise en place d'un cadre harmonisé des services dits de confiance dont la signature électronique dite avancée. Le Règlement renforce en particulier le principe d'équivalence juridique entre la signature électronique et la signature manuscrite (art. 25).

Ces évolutions conduisent à questionner l'impact réel ou supposé de la dématérialisation sur le droit de la preuve, au travers de ces différentes applications techniques. A cette fin sera d'abord étudiée la notion de copie numérique en l'appréciant à l'aune de la condition de fidélité. La fidélité est désormais la seule exigence retenue dans le projet d'ordonnance portant réforme du droit des contrats, du régime général et de la preuve des obligations de novembre 2014, le texte proposant de supprimer la condition de durabilité de la copie. Cette recherche devra notamment intégrer les propositions du rapport du Groupe de travail AFNOR *Numérisation fidèle* remis en juin 2015. Cette analyse conduira en particulier à comparer les deux approches de la notion de fidélité : formelle et informationnelle. Par ailleurs, la thèse se penchera sur la signature électronique (simple ou avancée, certificats qualifiés de signature électronique), cette dernière établissant un rapport entre une personne et un document. Enfin, et de manière plus large, elle cherchera à mesurer les différentes conséquences juridiques et judiciaires liées à la dématérialisation des contenus. La dimension européenne et l'apport comparatiste, par l'étude de droits étrangers, seront à privilégier.

Direction de Thèse :
Linda ARCELIN-LÉCUYER, maître de conférences HDR, et André GIUDICELLI, Professeur des universités.

Les candidats devront être titulaires d'un Master 2 à la date de la signature de leur contrat. Les candidatures, accompagnées d'un CV et d'une lettre de motivation, seront envoyées uniquement par voie numérique, en fichier PDF, entre le 10 et le 30 juin 2015, au secrétariat du CEJEP, à l'adresse suivante : berenice.gentet@univ-lr.fr

Note

Le projet SHADES est un projet interdisciplinaire portant sur la sécurité des documents, en partenariat avec des acteurs et des chercheurs des domaines de l'informatique et du droit. L'objectif de ce projet est de fournir un nouvel outil permettant l'authentification de l'intégrité du contenu d'un document par le biais du calcul d'une signature robuste et compacte afin de lutter contre la fraude et la falsification. Cette signature « sémantique » sera basée sur le contenu (textuel et graphique) du document et prendra également en considération la structure interne sous-jacente aux éléments de base composant ce document (relations spatiales). Grâce à un hachage de l'information du document lors du calcul de cette signature, aucune information du document original ne pourra être déduite de sa seule signature. La signature pourra alors être insérée dans le document ou utilisée dans un logiciel de gestion de contenu d'entreprise afin de vérifier l'authenticité du document, sans toutefois compromettre sa confidentialité. En outre, cette signature basée sur le contenu pourra permettre plusieurs niveaux de sécurité, comme la copie conforme d'un document et la copie fidèle au contenu d'un document (le même contenu, mais pas la même disposition). Cette étude méthodologique et technologique sera complétée par une étude sur les aspects juridiques de cette nouvelle technologie et son intérêt pour les professionnels du droit. Le projet sera réalisé en collaboration avec un tiers de confiance comme utilisateur final.