La récolte transfrontière de preuves électroniques dans le contexte européen
Construction d'un modèle à l'aune d'une nouvelle conception de la souveraineté des Etats

Résumé (court) de la thèse de doctorat

1. Les preuves électroniques sont devenues un enjeu crucial dans le cadre des enquêtes pénales. Leur intérêt est directement lié à l'utilisation intensive des technologies de l'information, qui impriment le quotidien de la majorité d'entre nous et dans le cadre desquelles des données – qui peuvent potentiellement constituer des preuves – sont générées.

Les preuves électroniques existent en effet dès lors que n'importe quel ordinateur, smartphone, tablette, clé USB ou autre composant informatique est utilisé, que ce soit pour faciliter la commission d'une infraction – traditionnelle ou de nature informatique – ou pour stocker ou transmettre certaines informations dont le contenu peut s'avérer déterminant dans le cadre de la résolution d'une investigation.

2. La récolte de ces preuves électroniques par les autorités en charge des enquêtes criminelles pose diverses questions. Celle qui a retenu notre attention dans le cadre de notre thèse de doctorat tient au fait que ces preuves se trouvent « dans le cyberespace ».

Un tel constat impose certaines réflexions relatives aux limites territoriales de l'intervention des autorités en charge des investigations, lorsque celles-ci souhaitent récolter des preuves électroniques. Généralement, les autorités d'enquête déploient en effet leurs pouvoirs d'investigation sur le territoire de l'Etat auquel elles ressortissent, tandis qu'elles sollicitent leurs homologues étrangères lorsqu'elles entendent obtenir des preuves qui se trouvent sur le territoire d'un Etat tiers. La démarche est essentielle pour assurer la souveraineté de cet Etat tiers, dont le respect interdit tout déplacement des autorités en charge d'une enquête en dehors des frontières nationales.

La récolte de preuves électroniques semble néanmoins mal s'accommoder d'un tel mode de fonctionnement.

3. Ainsi, par exemple, les autorités d'enquête peuvent être confrontées à une affaire de *Ransomware,* dans le cadre de laquelle le système informatique d'une entreprise espagnole aurait été piraté, permettant au pirate informatique de s'emparer d'informations sensibles et d'extorquer ensuite des fonds auprès de la société en brandissant la menace de diffuser ces informations dans le monde entier, à défaut de recevoir satisfaction.

Les autorités compétentes chercheront alors à démasquer l'auteur des faits en tentant d'identifier l'utilisateur d'une adresse IP spécifique. Si l'adresse IP utilisée renvoie à l'Ukraine, les autorités espagnoles pourraient ainsi vouloir s'adresser directement à un fournisseur d'accès à Internet ukrainien aux fins d'obtenir l'identité de l'utilisateur de l'adresse IP, sans devoir passer par les étapes de la procédure applicable en matière de coopération judiciaire. Le temps que les autorités ukrainiennes réagissent, il se pourrait en effet que les informations relatives à l'utilisateur n'aient pas été conservées par le fournisseur de services, rendant toute tentative d'identification du pirate informatique impossible alors que ce dernier aura peut-être extorqué des milliers d'euros à l'entreprise espagnole.

Une situation similaire pourrait également se présenter si les autorités espagnoles, ayant identifié le suspect, souhaitaient prendre connaissance de ses communications électroniques en s'infiltrant, en secret, dans son ordinateur aux fins d'y effectuer une recherche informatique à distance. Une telle technique – qui s'apparente également à un piratage informatique – est autorisée par certaines législations nationales. Celle-ci peut s'avérer plus simple et plus efficace que de s'adresser aux autorités ukrainiennes en vue de leur demander de saisir ces informations en procédant à une recherche portant – directement cette fois – sur l'ordinateur du suspect qu'elles auront préalablement dû – physiquement – localiser, en espérant que les communications pertinentes n'aient pas, entretemps, été effacées.

Les autorités ukrainiennes, qui seraient contactées aux fins d'assister les autorités espagnoles dans leur investigation, pourraient en outre ne pas disposer, sur la base de leur droit national, des mesures d'enquête qui leur permettraient de saisir les données informatiques sur leur propre territoire. Elles peuvent également manquer de la capacité technique utile à l'exécution de la mesure sollicitée ou répondre à la demande seulement après plusieurs mois. Il est également possible qu'elles n'entendent pas répondre (positivement) à la demande qui leur serait adressée pour des raisons exclusivement diplomatiques.

Pour le surplus, si les autorités espagnoles ont pu, dans notre exemple, identifier les autorités ukrainiennes comme étant susceptibles de les assister dans la récolte de preuves électroniques, il y a également certaines situations qui ne permettent pas de déterminer l'endroit où la mesure d'enquête visant à récolter les preuves électroniques devrait être mise en œuvre.

4. La question de savoir comment les autorités en charge des enquêtes doivent se comporter face à la composante internationale qui caractérise les différentes situations évoquées est une question cruciale pour pouvoir assurer la récolte efficace des preuves électroniques, tout en assurant le respect de la souveraineté des Etats tiers.

L'ambition de notre recherche doctorale a été d'apporter des solutions à ces situations, en construisant un modèle de récolte de preuves électroniques suffisamment élaboré pour rencontrer ce double objectif et résolument pratique afin de pouvoir être utilisé par les autorités des Etats membres de l'Union européenne.