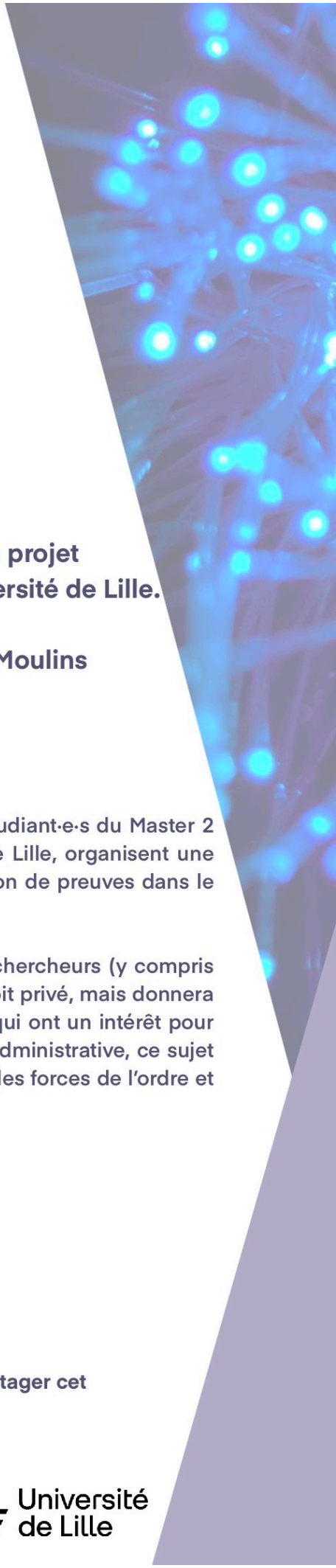
Appel à communication

Cybersurveillance, enquêtes et preuve électronique

Droits et libertés à l'épreuve du déchiffrement



Journée d'étude organisée par l'équipe de recherche en droit du projet européen EXFILES et le Master 2 droit du cyberespace de l'Université de Lille.

Faculté des sciences juridiques, politiques et sociales, Campus Moulins
1, place Déliot, 59000 Lille

Le vendredi 9 juin 2023, de 9h à 17h30

L'équipe de recherche en droit du numérique du CERAPS (UMR 8026) et les étudiant·e·s du Master 2 de droit du cyberespace de la Faculté de Sciences Politiques et Juridiques de Lille, organisent une journée d'étude sur le thème du déchiffrement des données à fins de production de preuves dans le cadre des enquêtes judiciaires et administratives.

Cette journée d'étude a vocation à réunir les interventions de chercheuses et chercheurs (y compris doctorant·e·s) de disciplines juridiques essentiellement, de droit public et de droit privé, mais donnera également la parole à des praticiens spécialisés en dehors de ces disciplines qui ont un intérêt pour ce sujet. En effet, au-delà des enjeux inhérents à la procédure pénale comme administrative, ce sujet conduit à des réflexions éthiques et sociétales plus larges quant aux pratiques des forces de l'ordre et à notre droit, que cette journée permettra d'explorer grâce à cette diversité.

Dates importantes :

Soumission du résumé **le 11 avril 2023**
Soumission de l'article **le 31 mai 2023**
Journée d'étude **le 9 juin 2023**

Nous vous invitons à inscrire ces dates dans vos agendas et à partager cet appel à communication au sein de votre réseau.

The EXFILES project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883156.

EXFILES

Université de Lille

Contexte de l'appel à communication

L'Observatoire des Libertés et du Numérique soulignait dans son positionnement « Chiffrement, sécurité et liberté » de janvier 2017 : « La capacité de chiffrer ses communications numériques et ses données informatiques est une condition indispensable à la préservation des droits et libertés fondamentales, et l'un des derniers remparts, individuels et collectifs, aux intrusions arbitraires et illégales de nombreux acteurs, étatiques, privés, ou criminels. Le chiffrement va bien au-delà d'une question de droits de l'Homme : alors que le numérique a investi l'ensemble des champs d'activité humains, l'affaiblir, [...], reviendrait à fragiliser considérablement l'économie, mais aussi la sécurité collective. »

Toutefois, dans un État de droit, le droit à la vie privée doit pouvoir coexister avec d'autres impératifs comme le maintien de l'ordre public et de la sécurité nationale. En effet, le chiffrement, aussi utile soit-il pour assurer le respect des droits fondamentaux, peut devenir un véritable enjeu lorsqu'il s'agit de produire des preuves devant un tribunal (dans un contexte administratif comme judiciaire) ou de veiller à la sécurité nationale par des techniques de surveillance. Tout l'enjeu actuel pour un État de droit sera donc d'organiser la production de preuves électroniques obtenues souvent après déchiffrement, soit dans le matériel saisi, soit par interception des télécommunications, tout en assurant le respect des droits et des libertés fondamentales des personnes.

Cette journée d'étude sera organisée en lien avec le projet européen EXFILES (Extract Forensic Information for Law Enforcement Agencies from Encrypted Smart Phones www.exfiles.eu), qui vise, depuis 2020, à développer une technique innovante, matérielle et logicielle, d'extraction des données chiffrées de smartphones dans le cadre d'enquêtes judiciaires, tout en ancrant cette réflexion dans une approche plus globale.
Ainsi, cet évènement a vocation à revenir sur les enjeux juridiques majeurs du chiffrement, des enquêtes transfrontalières, et de la preuve électronique face aux libertés et droits fondamentaux, mais aussi d'élargir nos réflexions à l'enquête administrative, à la sécurité nationale dans un contexte européen et international (au cœur d'actualités comme l'affaire Pegasus), ou encore aux frontières que connaît notre droit et que le cyberespace ignore.

Toutes les propositions d'intervention sur ces sujets sont les bienvenues et seront étudiées avec attention.

Les interventions seront réparties selon deux axes : le renseignement dans un contexte préventif et de sécurité nationale sera l'objet des discussions de la matinée, la preuve dans l'enquête judiciaire sera le fil conducteur de l'après-midi. Les interventions attendues seront limitées à 25 minutes, et suivies de tables rondes afin de favoriser les échanges entre les participants.

Modalités de candidature **:**

Les propositions de contributions sont à envoyer au plus tard le 11 avril 2023 à l'adresse suivante :

colloque-cyberdroit@univ-lille.fr.

Cette proposition de contribution consiste en un résumé du propos qui sera présenté, limité à 2 pages (ou environ 1000 mots hors notes de bas de page et bibliographie), en français uniquement. Une réponse sera donnée aux candidats le 21 avril au plus tard. Les autrices et auteurs dont la contribution est sélectionnée après une évaluation anonymisée devront envoyer leur article complet au plus tard le 31 mai 2023.

Les propositions de contribution ne doivent pas comporter de références personnelles dans le texte ou sur le document, les noms et affiliations des auteurs et autrices devront être mentionnés dans l'e-mail qui l'accompagne, afin de respecter le processus de relecture anonymisée.

Les interventions feront l'objet d'une publication ultérieure (éditeur en cours de discussion).

Pour vos questions, merci de contacter colloque-cyberdroit@univ-lille.fr, ou audrey.dequesnes@univ-lille.fr.