fundazione
Università di Corsica
Pasquale Paoli

Università di Corsica Pasquale Paoli
ÉQUIPE MÉDITERRANÉENNE DE RECHERCHE JURIDIQUE UR 7311

CHAIRE
CONFIANCE NUMÉRIQUE

«Cybersécurité et confiance numérique»

VENDREDI 21 JANVIER 2022 DE 14H À 17H

AMPHI ETTORI , CAMPUS MARIANI

RESPONSABLES SCIENTIFIQUES :

ANDRÉ GIUDICELLI
PROFESSEUR DE DROIT PRIVÉ ET SCIENCES CRIMINELLES À L'UNIVERSITÉ DE CORSE

ERIC CAPRIOLI
AVOCAT À LA COUR DE PARIS, DOCTEUR EN DROIT, MEMBRE DE LA DÉLÉGATION FRANÇAISE AUX NATIONS UNIES

INTERVENANTS :

XAVIER LEONETTI
MAGISTRAT, CHEF DE LA MISSION DE PRÉVENTION ET DE LUTTE CONTRE LA CYBERCRIMINALITÉ, DIRECTION DES AFFAIRES CRIMINELLES ET DES GRÂCES, MINISTÈRE DE LA JUSTICE

PHILIPPE CLERC
CONSEILLER EXPERT POUR LES ÉTUDES ET LA PROSPECTIVE, CCI FRANCE. PRÉSIDENT DE L'ACADÉMIE DE L'INTELLIGENCE ÉCONOMIQUE

JEAN-PAUL MATTEI
MAÎTRE DE CONFÉRENCES ASSOCIÉ À L'UNIVERSITÉ DE CORSE, AVOCAT

PIERRE-DOMINIQUE CERVETTI
MAÎTRE DE CONFÉRENCES À AIX-MARSEILLE UNIVERSITÉ, AVOCAT. DIRECTEUR DE LA CHAIRE INNOVATION ET BREVETS

EN PARTENARIAT AVEC :
fntc

ENTRÉE LIBRE SUR PRÉSENTATION DU PASSE SANITAIRE

fundazione.universita.corsica

FUNDAZIONE
UNIVERSITÀ DI CORSICA PASQUALE PAOLI
fondation@univ-corse.fr
04 20 20 21 55

CHAIRE CONFIANCE NUMÉRIQUE
6ème édition
21 Janvier 2022 de 14h à 17h
«Cybersécurité et confiance numérique»
Amphi Ettori

Propos introductifs : **ANDRÉ GIUDICELLI, Professeur de droit privé et sciences criminelles à l'Université de Corse, Directeur de l'Équipe méditerranéenne de recherche juridique, co-responsable scientifique de la Chaire Confiance numérique.**

Xavier Leonetti, Magistrat, chef de la Mission de Prévention et de Lutte contre la cybercriminalité, Direction des affaires criminelles et des grâces, Ministère de la Justice :
La gestion judiciaire d'une cybercrise

Docteur en droit, ancien officier de gendarmerie (chef du service de la sécurité économique de la direction générale), Xavier Leonetti est à présent magistrat, chef de la mission de prévention et de lutte contre la cybercriminalité (après avoir exercé au sein de la JIRS Economique et financière de Marseille). Il est notamment l'auteur de : La France est-elle armée pour la guerre économique ?, Armand Colin (2011), Le Petit RGPD, Dunod (2021), Smartsécurité et CyberJustice, Puf (2021).
Son intervention se concentrera sur la gestion judiciaire d'une cybercrise et sur les moyens permettant aux entreprises et aux particuliers d'aborder les grands évènements, tels que les JO 2024, avec confiance.

Philippe CLERC, conseiller expert pour les études et la prospective, CCI France. Président de l'Académie de l'intelligence économique *:*
La confiance, enjeu majeur du partage des données numériques pour les PME.
État des lieux et perspectives.

La révolution numérique actuelle constitue une profonde mutation des modes de production, de commercialisation de consommation et de travail. Elle ouvre les perspectives d'une nouvelle croissance plus écologique. Mais elle inaugure aussi une ère de vulnérabilités et de risques considérablement augmentés. Interconnectés ceux-ci engendrent progressivement des cyber-crises systémiques aux enjeux politiques, économiques et sociétaux inédits. Les activités cybercriminelles s'industrialisent. Leur origine se situe dans l'ordre inter-étatique, comme dans l'ordre mafieux et criminel. Les entreprises sont une cible privilégiée, plus encore les PME et les TPE. En effet, leurs dirigeants peinent à investir dans une sécurité dont l'aspect multidimensionnel les rebutent. La confiance numérique s'impose comme défi central pour dépasser cet état. Comme contribution à l'organisation d'actions destinées à instaurer la confiance, nous présenterons les résultats de deux études innovantes, conduites par CCI France dans le cadre de la mission consultative nationale des CCI, l'une sur l'échanges des données d'entreprises, l'autre sur l'anticipation des risques et la cyberrésilience.

Jean-Paul MATTEI, Maître de conférences associé à l'Université de Corse, avocat *:*
L'influence sociale, nouvel enjeu de la cybersécurité ?

La « cybersécurité » concerne les usages défensifs et offensifs des systèmes d'information qui irriguent désormais nos organisations modernes. Elle est en quelque sorte le miroir des formes de plus en plus nombreuses et complexes de la cybercriminalité.
C'est pour cela que nous sommes tous plus ou moins aujourd'hui familiers des risques que représentent les attaques de type : hacking, spoofing, carding, skimming, scamming, spamming, cryptologie, google bombing, cracking, fraudes aux enchères, etc.
Mais il semble aujourd'hui nécessaire de relever également que « Les cyberattaques les plus sophistiquées et les plus dévastatrices commencent souvent par des cyberattaques d'ingénierie sociale, telles que le spear phishing, où l'attaquant accède à un réseau d'entreprise » (Hutchins et al., 2011).
De façon beaucoup plus pernicieuse, et comme l'observe la journaliste Maria Ressa, Prix Nobel de la paix 2021, nous vivons dans l'ère des autoritarismes numériques qui se distinguent notamment par « une manipulation

insidieuse de l'attention humaine, de nos émotions, pour créer des réalités alternatives. »
Ce phénomène n'est pas nouveau, il est d'ores et déjà répertorié dans le texte fondateur de la doctrine française du SGDN de 2018, fixant le cadre du modèle français de cyberdéfense au titre des tentatives de déstabilisation, repérées lors des élections américaines ou des printemps arabes.
Comment ne pas interroger la notion de souveraineté cyber à l'aune de cette nouvelle approche de l'influence ?»

Pierre-Dominique CERVETTI, Maître de conférences à Aix-Marseille Université, avocat, Membre du Centre de droit économique (EA 4224) et Directeur de la Chaire Innovation et Brevets.
La souveraineté numérique : un enjeu majeur du XXIe siècle

La question de la souveraineté numérique est présente au cœur des débats portant sur la gouvernance mondiale de la société de l'information. Celle-là même qui a vu, à travers l'essor du numérique, l'expansion des GAFAM et l'avènement d'un système de création de valeur par la captation, le traitement et la commercialisation des données personnelles.
Le succès des réseaux sociaux induit un brouillage des frontières entre l'espace public et la sphère privée. L'accumulation des données privées (dans ce qu'il est convenu de nommer le Big Data) représente, certes, une richesse commerciale pour les entreprises qui les maîtrisent, mais elle est tout autant le vecteur de potentialités pour le secteur public, pouvant être utilisées à des fins collectives.

Propos conclusifs : **Eric CAPRIOLI, avocat, docteur en droit HDR, co-responsable scientifique de la Chaire Confiance numérique.**