APPEL À PROJETS #2

Ouverture 01.10.2024 | Clôture 07.02.2025

Cet appel à projets vise à stimuler l'innovation collaborative afin de proposer des solutions contribuant à relever les défis liés à la sécurité des contenus multimédias, allant de la confidentialité des données jusqu'aux menaces émergentes liées aux nouvelles technologies. Il est mené en collaboration avec Initiative for Media Innovation (IMI).

Nous invitons les chercheurs des Hautes Ecoles, les acteurs de l'industrie du multimédia et de la presse, les experts en technologies digitales et les partenaires de l'innovation à joindre leurs efforts en quête de protection des données et de sécurisation des échanges multimédias dans le paradigme de profonde mutation des canaux d'informations et des interrelations humaines.

CONTEXTE ET ENJEUX

Depuis de nombreuses années, l'information à travers le multimédia prend une ampleur considérable, avec l'avènement des médias en ligne, puis avec celui des réseaux sociaux et des objets connectés et enfin celui du travail et de la communication à distance depuis la crise sanitaire. Ainsi, l'image, le texte et le son sont devenus les principaux vecteurs de communication au sein de la société.

Ce changement de paradigme impacte directement la notion de sécurité à différents niveaux. La cybersécurité joue ainsi un rôle-clé pour rétablir la confiance, par exemple en préservant la confidentialité du contenu, en garantissant son origine, en permettant sa traçabilité ou en certifiant son intégrité.

1

Protection de la sphère privée

En quelques années, notre exposition personnelle en ligne a massivement pris de l'ampleur, en corrélation directe avec l'intensification de l'usage des réseaux sociaux et autres plateformes numériques. Une partie substantielle de la vie privée des individus est désormais accessible sur Internet (photos/vidéos, localisation géographique, CV, etc.). Nos données biométriques, requises par toujours plus d'applications (authentification par reconnaissance faciale ou vocale particulièrement), sont particulièrement sensibles. Des mesures robustes de protection des données personnelles, mais aussi de la propriété intellectuelle et/ou commerciale (par ex. pour des photos et des vidéos), sont donc impératives.

2

Sécurisation des communications privées

Les constantes évolutions technologiques imposent de renforcer les techniques de sécurisation des canaux d'information et des communications. Celles-ci doivent être à même de garantir, en tout temps, l'authenticité et la confidentialité. Cette nécessité est particulièrement avérée par le déploiement massif de la visioconférence, mais plus généralement aussi par les échanges d'emails et autres interactions électroniques (sur les réseaux sociaux et avec des objets connectés notamment). Il s'agit même d'un facteur critique si l'on observe l'implémentation de modèles d'intelligence artificielle (IA) basés sur l'analyse et la classification d'images pour prendre des décisions (par ex. dans les véhicules autonomes).

3

Protection contre les risques de désinformation publique

Plus que jamais, les émetteurs et diffuseurs d'informations doivent démontrer leur intégrité et leur authenticité face à un afflux d'informations potentiellement manipulées au travers des médias électroniques, réseaux sociaux et autres chaînes digitales. Pour la majorité de l'audience, il devient en effet de plus en plus compliqué de discerner avec justesse la vérité et la manipulation, et donc de se forger une opinion objective. La protection contre les risques de désinformation, plus particulièrement par la détection de falsification d'images et de voix (*deepfakes*), présente ainsi un enjeu considérable pour la société civile, dont la réponse fait appel aussi bien à des compétences en ingénierie informatique qu'en sciences sociales.

OBJECTIFS

L'objectif de cet appel à projets est de **prospecter de nouvelles idées et méthodes, d'étudier des concepts disruptifs et de développer des solutions techniques innovantes favorisant la confiance, la sécurité et la protection de la vie privée dans le domaine multimédia**, plus particulièrement :

- Développement de solutions technologiques pour garantir la sécurité des données multimédia, leur intégrité, leur authenticité et leur confidentialité (chiffrement, stéganographie, mécanismes de détection et de protection contre la falsification)
- Conception de mécanismes de protection contre les atteintes à la sphère privée dans un environnement multimédia (anonymisation des données, gestion des consentements, minimisation de la collecte d'informations personnelles)
- Exploration d'approches innovantes pour détecter et contrer les menaces potentielles dans le domaine du multimédia (contenus malveillants, usages abusifs, cyberattaques)

Les projets attendus s'inscrivent notamment dans les domaines suivants (non-exhaustif) :

- Tatouage d'images, de sons et de vidéos – *watermaking* – et autres mesures de certification de l'information à la source
- Détection, analyse et référencement des manipulations de contenus multimédia – *deepfakes* (algorithmes de reconnaissance, patterns, modes de diffusion/amplification)
- Caractérisation des attaques et développement de protections d'algorithmes de *machine learning* pour la classification d'images
- Gestion des données biométriques (reconnaissance faciale, biométrie comportementale)
- Détection d'usurpation de voix et contre-mesures

CONTACT

Pour toute demande de renseignement ou besoin d'accompagnement pour initier un projet, veuillez prendre contact avec :

Sandy Wetzel
Responsable du Programme **[seal]**
+41 78 761 23 36
contact@seal-innovation.ch