



Le métavers, nouveau terrain de jeu des criminels

publié en décembre 2025

Économie & Services Focus Sur Six Recherches N°30

À l'ère des mondes virtuels, la criminalité se transforme en harcèlement immersif, escroqueries 3D ou usurpation d'identité. Face à ces défis, un projet neuchâtelois ambitionne d'équiper les forces de l'ordre pour enquêter dans ces univers parallèles.

TEXTE | Grégory Tesnier

« L'essor de technologies puissantes comme le métavers rend le paysage criminel

encore plus complexe et transnational. » Lorsque Jürgen Stock, ancien secrétaire général d'Interpol – organisation qui coordonne la coopération policière au niveau international –, évoque les dangers liés au métavers, il souligne l'ampleur de la tâche qui attend les services chargés de l'application de la loi. C'est dans ce contexte qu'a vu le jour le projet M-Crime, lancé par l'Institut de lutte contre la criminalité économique (ILCE) de la [HE-Arc Gestion \(HEG Arc\) – HES-SO](#) à Neuchâtel. Son objectif : acquérir des connaissances solides afin de constituer un pôle de compétences en Suisse romande, spécialisé dans la lutte contre cette criminalité « métaversisée », expliquent en substance [Renaud Zbinden](#), adjoint scientifique à l'ILCE et porteur du projet, ainsi que [Luca Brunoni](#), maître d'enseignement à l'ILCE.

Le métavers ? Un environnement en ligne tridimensionnel où des utilisatrices et des utilisateurs, représentés par des avatars, interagissent dans des espaces virtuels éloignés du monde physique. Dans cet univers immersif, on peut travailler, jouer, créer ou interagir sous une même identité en ligne. Ce qui relevait hier de la science-fiction – pensons au film *Ready Player One* de Steven Spielberg (2018) – se concrétise déjà avec des plateformes



Le spécialiste Renaud Zbinden souligne la difficulté de

comme Horizon Worlds, Roblox, Fortnite, Minecraft, Decentraland ou TheSandbox. Certes, les attentes

mener efficacement une enquête lorsque les serveurs informatiques se trouvent à l'étranger. | © GUILLAUME PERRET

économiques du début des années 2020 ne se sont pas réalisées et « l'écosystème métavers » n'a pas encore trouvé sa forme définitive et rentable. Pour autant, les initiatives existantes ne sont pas anecdotiques : elles constituent déjà des laboratoires technologiques où s'expérimentent innovations... et dérives criminelles. Dans cette perspective, si le métavers venait à s'imposer auprès de larges publics, ses implications – techniques, juridiques et économiques – appelleraient une vigilance accrue de la part des autorités policières.

Outiller les enquêtes criminelles de demain

Le projet M-Crime, conduit par l'ILCE avec le soutien de la Police cantonale de Genève et de l'Université du Québec à Trois-Rivières, ambitionne dès lors de comprendre ce qui se passe dans ces mondes virtuels pour préparer les enquêtes criminelles de demain. « Beaucoup de phénomènes criminels que nous observons dans le métavers existent également hors du métavers », soulignent Renaud Zbinden et Luca Brunoni. L'environnement immersif ne crée pas une criminalité entièrement nouvelle – même si certains parlent déjà de « métacrime » – mais transforme celle qui existe déjà. Le harcèlement en ligne, par exemple, prend une ampleur inédite lorsqu'il s'exerce à travers un casque de réalité virtuelle ou une combinaison équipée de capteurs. D'autres formes d'actions répréhensibles évoluent également: usurpation d'identité, escroqueries financières, atteintes à la réputation ou manipulations psychologiques.

À mesure que les usages du métavers progressent, les défis se multiplient. Juridiquement, il ne s'agit pas d'un espace unique mais d'une constellation de plateformes privées, souvent basées à l'étranger, chacune avec ses propres caractéristiques. Les enquêtrices et enquêteurs doivent composer avec des juridictions multiples et des entreprises qui ne partagent pas toujours leurs données. « Comment conduire efficacement une enquête quand les serveurs informatiques sont hors de Suisse ? » s'interrogent Renaud Zbinden et Luca

Brunoni. La difficulté est aussi technique. Où se trouvent les traces exploitables ? Sur l'équipement de l'utilisateur ou de l'utilisatrice ? Sur des serveurs distants ? Certaines plateformes enregistrent scrupuleusement les interactions, d'autres n'en conservent que des fragments. Le métavers est enfin un univers social, avec ses codes et ses microcultures. Les novices deviennent des victimes privilégiées. Leur vulnérabilité se révèle autant sur le plan cognitif que technique.



En octobre 2022, Interpol a lancé son métavers, un espace dédié aux rencontres professionnelles, à la formation des forces de l'ordre et à l'anticipation des cyber crimes émergents dans les environnements immersifs. Ci-dessus, Jürgen Stock, l'ancien secrétaire général d'Interpol, expérimente le dispositif. | © INTERPOL

Formation des forces de l'ordre

Face à ces incertitudes, M-Crime adopte une approche exploratoire et pragmatique. Première étape : dresser un état des lieux du métavers – technologies, plateformes, usages actuels et futurs – enrichi d'entretiens avec des expertes et des experts, ainsi qu'avec les forces de l'ordre, en particulier la Police cantonale de Genève. Deuxième étape : analyser le cadre juridique, en confrontant les règles et la

jurisprudence aux pratiques observées. L'équipe mène aussi – troisième étape – des études de cas concrètes, en partenariat avec l'Université du Québec à Trois-Rivières, afin d'identifier les défis et les solutions. Enfin, les résultats seront synthétisés sous la forme d'un rapport global et d'un workshop destiné aux forces de l'ordre suisses. « Nous souhaitons voir concrètement comment une enquête peut être menée dans un environnement immersif », résument les chercheurs. Aujourd'hui, M-Crime a déjà parcouru un tiers du chemin et espère livrer ses résultats en 2026.

Mots-clés / Expert·es

Autorité BRUNONI Luca Données Économie HE-Arc Gestion (HEG Arc) Internet

ZBINDEN Renaud