Droits et devoirs

« Darkverse » : le côté obscur du métavers

Alain Bensoussan

A l'instar du darkweb, le « darkverse », face cachée du métavers, pourrait alimenter, comme le montre une étude récente, une nouvelle industrie criminelle bien plus malveillante encore. En outre, le contrôle illimité par les opérateurs de métavers remettrait en question la notion même de vie privée. Une chose est sûre : cette nouvelle ère de l'internet soulève de nombreux défis qui inquiètent les experts de la sécurité.

Phishing, ransomwares, chantage, usurpation d'identité… On connaît les dangers du dark web qui vont eux aussi se décliner dans le métavers, sans doute de façon beaucoup plus dangereuse.

En effet, dans le « darkverse », les cybercriminels vont pouvoir coordonner et mener des activités illégales en toute impunité car plusieurs années vont s'écouler avant que l'on puisse maintenir l'ordre et la sécurité sur ces nouveaux « territoires virtuels ».

Darkverse : vers une nouvelle industrie cyber criminelle ?

Les espaces métavers pourraient, dans les prochaines années, s'accompagner d'une criminalité spécifique plus difficile encore à appréhender que dans le darkweb. En effet, contrairement à ce dernier, le darkverse existe à l'intérieur du métaverse et n'est pas indexé. Il n'est donc pas consultable par les moteurs de recherche standard. C'est ce qui ressort d'une étude publiée cet été par Trend Micro, pionnier des antivirus et leader mondial de la cybersécurité (1).

Tour d'horizon des menaces « critiques »

Les premières menaces auxquelles on peut s'attendre visent les NFT, ces jetons non fongibles émis et échangés par la blockchain. Utilisés pour attester de la propriété d'actifs numériques, ils sont une composante importante du métavers. Devenus très populaires et lucratifs (2), ils pourraient être la cible de diverses attaques.

Si leur contenu ne peut pas être modifié, les NFT présentent néanmoins des fragilités qui les rendent vulnérables aux attaques à travers notamment les liens de téléchargement des fichiers de données. Si ces derniers sont cryptés lors d'une attaque de rançongiciel, l'utilisateur conservera toujours la propriété, mais il pourra être empêché d'accéder à ses actifs s'il ne paie pas une rançon.

Ce n'est hélas pas la seule fragilité. Un chercheur en sécurité a pu démontrer comment falsifier des illustrations NFT en parvenant à créer des œuvres qui

changent en fonction de l'adresse IP du spectateur et de la plateforme NFT. Il a réussi à faire un NFT qui change en fonction de l'endroit d'où il est regardé[3]. Bon nombre des NFT ainsi transformés pourraient être considérés comme des contrefaçons. .

Les activités illégales ou criminelles sont également susceptibles de prospérer dans le darkverse car il sera difficile à surveiller et à infiltrer sans jeton d'authentification. Les forces de l'ordre pourront difficilement exercer un contrôle efficace dans ces espaces non seulement en raison du coût élevé des interceptions à grande échelle dans les métaverses, mais également parce qu'elles auront besoin de temps pour développer leur expertise en la matière.

Les fraudes financières constitueront une autre menace. Les groupes criminels seront attirés par le métaverse en raison des énormes volumes de transactions induites par cette nouvelle économie numérique. Le blanchiment d'argent se fera par les NFT (y compris contrefaits) et les biens immobiliers surévalués dans le métavers.

Par ailleurs, les métavers sont susceptibles de remettre en question la protection de la vie privée et des principes l'encadrant.

La protection de la vie privée remise en cause

La notion de vie privée devra être reconsidérée car les opérateurs de ces environnements virtualisés auront une visibilité sans précédent sur les actions des utilisateurs. En fait, la notion de vie privée telle que nous la connaissons sera profondément remise en question dans ces univers en immersion totale. Le métavers réduit en effet la capacité individuelle à échapper à la collecte de données[4].

En outre, des questions inédites risquent d'être soulevées en raison des nouvelles catégories de données personnelles générées (expressions faciales, gestes, réactions produites dans les interactions entre avatars). Celle-ci permettront aux opérateurs de métavers de mieux comprendre les processus de pensée des utilisateurs et ouvriront la possibilité d'un profilage renforcé.


© Cottonbro / Pexels.

Enfin, de par la quantité inédite de données susceptibles d'être collectées, l'application concrète des principes posés par le Règlement Général sur la Protection des Données (RGPD), notamment l'information et le consentement des utilisateurs, constitue un autre défi de taille.

A surveiller

Ce ne sont bien sûr que des projections car il est difficile d'estimer à ce stade, le nombre de questions que vont soulever ces mondes virtuels fictifs.

Aussi, tout comme il a fallu réglementer l'usage d'internet lorsque les contentieux se sont développés, il faudra encadrer les métavers[5] afin que soit placé, en exergue de toute réglementation positive, le principe des droits de l'homme numérique[6].

Seule une réflexion approfondie sur les métavers permettra d'anticiper efficacement les enjeux juridiques, économiques et sociaux majeurs qui se profilent au cours des prochaines années.

Alain Bensoussan

(1) Trend Micro Research, Metaverse or metaworse? Cybersecurity threats against the internet of experiences, N. HUQ, R. REYES, Ph. LIN, and M. SWIMMER, August 08, 2022.
(2) Un NFT de l'œuvre numérique « Everydays : The First 5000 Days » de l'artiste numérique américain Beeple a été vendu aux enchères par Christie's pour 69,3 millions de dollars en mars 2021.
(3) Moxie Marlinspike, cité par Trend Micro Research, précité.
(4) Cnil, « Métavers : réalités virtuelles ou collectes augmentées ?», LINC du 5 novembre 2021.
(5) Cf. notre chronique Droits et devoirs PR n°72, mars-avril 2022.
(6) Livre blanc des droits de l'homme numérique », Groupe de travail présidé par A. Santini et A. Bensoussan, novembre 2000.