INGÉRENCE ÉTRANGÈRE ET JEUX VIDÉO EN EUROPE : JOUER EST-IL POLITIQUE ?

Ophélie OMNES et Pierre MALVOISIN

Cabinet OMNES Legal & Positive Lobbying

« L'UE doit mieux lutter contre l'ingérence étrangère et la désinformation. »[1] C'est la conclusion inquiétante tirée par la résolution du Parlement européen, votée à l'immense majorité en mars dernier. Depuis, les exemples qui confirment le constat de l'assemblée européenne sont légions. De l'interdiction de Russia Today et Sputnik au début de la guerre en Ukraine, au « Qatargate » au Parlement européen début décembre 2022, le phénomène d'ingérence étrangère auquel est soumise l'Union européenne n'en finit pas de se manifester.

Définie comme l'intervention d'un État dans les affaires intérieures d'un autre État[2], l'ingérence étrangère n'est pas, en soi, un phénomène nouveau[3]. Ce qui semble plus récent, et rampant, c'est la volonté affichée d'acteurs étrangers de plus en plus influents sur la scène internationale de s'immiscer dans les mécanismes démocratiques occidentaux dans le but de les déstabiliser. Cette ingérence stratégique se manifeste par la volonté d'alimenter une propagande de nature complotiste et d'influencer les pensées et les comportements. La volonté, si elle n'est pas toujours affichée, est souvent la même : s'attaquer au modèle de démocratie occidentale (et souvent dite « libérale »). Parmi les acteurs identifiés et récurrents, on compte des puissances étrangères comme la Russie et la Chine, et plus récemment le Qatar, qui ont participé à des cyberattaques, à des soutiens financiers et à des coercitions économiques, mais aussi à de la manipulation de l'information en ligne, allant parfois jusqu'à influencer les processus démocratiques, tels que le vote sur la sortie du Royaume-Uni de l'Union européenne ou l'élection de Donald Trump aux Etats-Unis en

---

[1] **KALNIETE Sandra**, Rapport sur *l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformatio*n, résolution adoptée par le Parlement européen le 9 mars 2022 : https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_FR.html

[2] « Ingérence ». 2012. In Portail lexical : lexicographie. Nancy, France : Centre national de ressources textuelles et lexicales (CNRTL). En ligne < https://www.cnrtl.fr/definition/ingérence>

[3] « Ingérence » CNRTL, cité ci-avant : *« Se protéger contre les ingérences extérieures. L'État préservé des ingérences de l'étranger (Doc. hist. contemp.,1946, p. 179). Affaires capitalistes. C'est l'un des secteurs auxquels l'on se réfère le plus généralement pour évoquer l'ingérence des intérêts étrangers dans la vie politique d'un grand nombre de pays (Meynaud, Groupes pression Fr.,1958, p. 324):*

... j'écrivis à Eden que moi-même et le Comité national avions décidé que Muselier n'était plus commandant en chef de la marine et que nous n'acceptions pas, à ce sujet, l'ingérence du gouvernement anglais. De Gaulle, Mém. guerre,1954, p. 222.

2016. Autant de faits permettent d'illustrer la fragilité de l'Union européenne face aux stratagèmes des puissances étrangères, visant à diviser les États membres.

Dans un monde ultra-connecté et partiellement dématérialisé, les tentatives d'ingérence passent notamment par l'utilisation ciblée des médias et des réseaux sociaux. Une grande partie se passe donc en ligne, où il est plus facile de brouiller les pistes des véritables commanditaires. Mais qui dit positionnement stratégique sur les réseaux sociaux, dit nécessairement investissement de la sphère du jeu vidéo.

Quand on parle de jeu vidéo, on imagine souvent, à tort, qu'est seulement concerné un paquet de quelques adolescents mal dans leur peau et peu à l'aise avec les relations sociales. Et on ne pourrait pas être plus loin de la réalité. Les chiffres dépeignent un tout autre tableau et mettent en évidence la diversité des joueurs de jeux vidéo, bien plus représentative de la richesse des profils dans nos sociétés. L'âge moyen des joueurs de jeu vidéo est de 31.3 ans, et 76% des joueurs de jeu vidéo ont plus de 18 ans. 47.8% des *gameurs* sont des femmes[4]. Pire, quand on parle du monde du jeu vidéo, on ne parle seulement de celles et ceux qui jouent activement, on parle aussi de tout l'écosystème qui gravite autour, et qui finit par toucher un public encore plus large. Mais s'il est une impression que l'on peut avoir qui est correcte, c'est que, parmi les joueurs exposés, il y a en fait pléthores de mineurs. En effet, 71% des 6-10 ans et 80% des 11-14 ans jouent à des jeux vidéo[5]. Et si ça n'est pas la seule raison valable pour se préoccuper de la manière dont on protège – ou non – le monde du jeu vidéo, c'en est à tout le moins une raison suffisante.

On parle donc d'une véritable communauté d'individus, d'âges et d'horizons variés, active sur des supports différents, qui représente 124,8 millions de joueurs en Europe, dont plus d'un tiers sont des mineurs[6].

Et pourtant, il semble que le jeu vidéo soit passé sous les radars politiques et qu'il continue à ne pas être considéré par les gouvernements européens, qu'ils soient nationaux ou communautaires, comme une cible privilégiée à protéger à tout prix pour éviter la propagation progressive, mais certaine, d'idées illibérales. Pas qu'il ne soit pas considéré du tout, mais il est encore perçu, de manière un peu traditionnel, comme un bien matériel et économique qu'il faut réglementer comme un produit ; au mieux commence-t-il progressivement à être envisagé comme un bien culturel. Mais à ce jour, il n'est toujours pas apprécié pour ce qu'il est devenu : un objet complexe, à la croisée des chemins entre divertissement, commerce, culture et politique. Ainsi, le 10 novembre 2022, le Parlement européen adoptait une résolution dans laquelle il souligne que *« les jeux vidéo et le sport électronique disposent d'un fort potentiel pour promouvoir davantage l'histoire, l'identité, le patrimoine, les valeurs et la diversité européens au moyen d'expériences immersives; estime qu'ils sont également susceptibles de contribuer au pouvoir d'influence de l'Union »*[7]. Le colégislateur européen énonce ainsi sa prise de conscience de l'existence d'un *soft power* de l'Union européenne par le biais des jeux vidéo, sans que nulle part ne soit adressé le problème inverse, à savoir que les autres puissances étrangères utilisent également (déjà !) ce *soft power* à leur avantage.

---

[4] **Europe's video games industry**, **European Games developer Federation**, *Key Facts from 2021*, publié en 2022, données Ipsos.
[5] *ibid*.
[6] *ibid*.
[7] Sport électronique et les jeux vidéo, 10 novembre 2022, point 16 de la résolution, disponible en ligne sur : https://www.europarl.europa.eu/doceo/document/TA-9-2022-0388_FR.html

La question qui se pose, c'est donc celle de savoir en quoi le jeu vidéo constitue d'ores et déjà, un canal d'ingérence puissant dont il est urgent de prendre conscience, afin d'éviter que les mesures prises contre l'ingérence par ailleurs ne se voient privées d'effet face à l'existence de réseaux souterrains. Autrement dit : au regard de l'étendu de l'industrie et de la vulnérabilité du public cible, comment identifier et lutter contre l'ingérence étrangère dans le jeu vidéo ?

Les activités numériques sont des dispositifs où fermente une certaine animosité sous couvert de l'anonymat en ligne. C'est ainsi qu'elles en deviennent un terrain fertile pour l'expression et le développement de la désinformation et de la haine en ligne, phénomène parfois stratégiquement alimenté par les puissances étrangères désireuses de déstabiliser les démocraties occidentales. Et nous verrons dans un premier temps en quoi le jeu vidéo, en ce qu'il est un élément de *soft power* qui touche un public beaucoup plus large qu'il n'y paraît, semble n'être qu'une inquiétante illustration de la diffusion de la propagande étrangère **(I)**.

Face à l'étendue du problème, les résolutions du Parlement européen, de même que les propositions de la Commission européenne, et les paquets législatifs récemment adoptés mettent en évidence un intérêt croissant de nos politiques pour les questions relatives à la protection du numérique. La guerre en Ukraine ayant renforcé ce sentiment, nous verrons néanmoins que le jeu vidéo comme cible de l'ingérence continue pour l'instant d'être dans l'angle mort de ces évolutions réglementaires **(II)**.

Enfin, nous nous attacherons à explorer quelques pistes de solutions envisageables à court et moyen terme pour renforcer la position du jeu vidéo comme cible de l'ingérence étrangère, du développement de l'architecture réglementaire, à la sensibilisation du grand public et notamment des joueurs plus jeunes **(III)**.

Notre étude aura donc pour objet de :

- Définir ce qu'on entend par « monde du jeu vidéo » afin de souligner l'ampleur du phénomène et l'urgence à s'y intéresser ;
- Constater la menace d'une ingérence étrangère, ou l'ingérence étrangère effective et réelle, dans le monde du jeu vidéo ;
- Mettre en évidence les effets de cette ingérence sur la population européenne, sur nos processus démocratiques et nos valeurs ;
- Analyser l'état de la réglementation – existante ou absente – relative au jeu vidéo comme objet social et politique ;
- Être force de proposition pour améliorer les normes actuelles, et en développer de nouvelles afin de renforcer le jeu vidéo comme un espace libre, inclusif et sécurisé ;

PARTIE I : UNE INGÉRENCE ÉTRANGÈRE DANGEREUSEMENT IMPLANTÉE DANS LE MONDE PROTÉIFORME DU JEU VIDÉO

Pour bien comprendre l'urgence à s'intéresser à un outil comme le jeu vidéo, il convient dans un premier temps d'appréhender toute sa complexité et sa diversité (1.) afin de saisir en quoi l'ingérence étrangère déjà bien en place dans sa sphère de gravitation (2.) et comment le jeu vidéo en est arrivé à devenir un intermédiaire des réseaux d'ingérence (3.).

1. La réalité autour du jeu vidéo : un écosystème très varié… et riche !

Il y a un réel risque à passer à côté du jeu vidéo comme objet de société. En effet, le jeu vidéo est bien plus pertinent et bien plus stratégique que l'on ne le croit ; son univers regroupe un ensemble de composants qui vont bien au-delà que ce que les préjugés peuvent nous laisser supposer.

Traditionnellement, le jeu vidéo peut être défini comme un jeu nécessitant un dispositif informatique, dans lequel un joueur agit dans un environnement virtuel. Il est possible de jouer à ces jeux sans connexion à un réseau, c'est-à-dire en « local ». Néanmoins, un nombre grandissant de jeux permettent également aux joueurs de jouer en ligne, et donc d'entrer en contact, d'interagir et de communiquer. Sous des sigles énigmatiques tels que « PvP » (*Player versus Player*, littéralement « Joueur contre Joueur ») ou « MMORPG » (M*assively Multiplayer Online Role-Playing Game* : « jeu de rôle en ligne massivement multijoueur »), se cachent une large communauté de joueurs qui communiquent, partagent et interagissent instantanément via des *tchats*, des messageries instantanées, des appels audios ou vidéos, directement intégrés aux jeux vidéo ou par le biais de plateformes intermédiaires (Discord, Skype, etc.).

[1.1. Tous les moyens mènent aux jeux vidéo]

La sophistication croissante des smartphones permet aujourd'hui d'également jouer, en ligne, directement depuis son téléphone. C'est d'ailleurs le mobile qui a complètement démocratisé le jeu vidéo. Selon une étude[8] menée par le Syndicat des Éditeurs de Logiciels de Loisirs (SELL), en collaboration avec Médiamétrie, spécialisée dans la mesure d'audience et l'étude des usages des médias audiovisuels et numériques en France, 54% des joueurs utilisent un smartphone pour jouer aux jeux vidéo, contre 44% avec une console de jeux TV et 21% avec une console de jeux portable.

[1.2. Le profil type de joueur n'existe pas]

[8] Étude réalisée du 24 août au 15 septembre 2022 sur Internet auprès d'un échantillon de 4001 internautes de 10 ans. Cette enquête a pour objectif de comprendre les usages et profils des joueurs de jeux vidéo en France. Disponible en ligne sur : https://www.sell.fr/sites/default/files/essentiel-jeu-video/lessentiel_du_jeu_video_nov_22.pdf

Dresser le profil type de ces "*gameurs"* (terme qu'on utilise dans les communautés de joueurs de jeux vidéo) est difficile… tout simplement parce qu'il n'y en a pas ! Tout le monde joue. Mais pas à la même chose. Ainsi, le jeu vidéo représente 37,4 millions de joueurs en France, parmi lesquels on dénombre 88% d'adultes (32,8 millions de joueurs) et ainsi 12 % de mineurs (enfants âgés de 10 à 17 ans, représentant 4,6 millions de joueurs). 53% de cet échantillon disent jouer régulièrement et ont une moyenne d'âge de 38 ans. Ils sont 53 % d'hommes et 47 % de femmes à jouer aux jeux vidéo au moins une fois par semaine. 95% des enfants de 10 à 17 ans jouent aux jeux vidéo.[9] Au niveau européen, on a compté 124,8 millions de joueurs en 2021, dont 52% ont entre 6 et 64 ans, avec une répartition par tranche d'âge relativement équitable et la plus grosse tranche d'âge de joueurs chez les... 45-64 ans ! (24%, contre 17% pour les 6-14 ans, 22% pour les 15-24 ans, 20% pour les 25-34 ans et 16% pour les 35-44 ans)[10]. La diversité des profils jouant aux jeux vidéo est flagrante. Il existe cependant en effet une large partie du public concerné qui se trouve être mineur, et donc nécessairement plus influençable et donc plus vulnérable quant à la diffusion d'idéologies générales.

[1.3. Un large marché de consommateurs qui génère bien des profits]

Le marché du jeu vidéo est donc un large marché de joueurs, et ainsi un large marché de consommateurs : en 2021, on estimait le marché européen de l'industrie du jeu vidéo à 23,3 milliards d'euros[11]. Considérer le jeu vidéo, c'est nécessairement s'intéresser à l'ensemble de la culture et des produits qui gravitent autour. C'est le cas du *streaming*, c'est-à-dire la technique permettant de diffuser et de lire en ligne un contenu en direct ou avec un léger différé, qui est très utilisé dans le domaine du jeu vidéo. Des plateformes telles que *Twitch*, *Omlet Arcade* et *Booyah Live* ont ainsi permis une augmentation considérable de l'engagement et de la monétisation du jeu vidéo : on peut désormais regarder derrière nos écrans des créateurs de contenus, c'est-à-dire des joueurs qui partagent en direct leurs performances. Ces *streamers* participent activement à mettre en avant de nouveaux jeux vidéo et à créer un esprit de communauté entre les différents *gameurs*. Cet esprit de communauté est souvent synonyme d'un partage de valeurs, comme en témoigne le *Z Event*[12], un marathon caritatif annuel réunissant des streamers francophones afin de récolter des dons et soutenir des associations caritatives. En 2019, après plus de 50 heures de streaming, les 57 personnalités du jeu vidéo et du divertissement en ligne ont récoltés plus de 10 millions d'euros : cette 7e édition détient le record mondial de

---

[9] *ibid*.

[10] **Europe's Video Games Industry** / **European Games Developer Federation**, *"Video games – A force for good - Key Facts from 2021"*, publié en 2022, données Ipsos.

[11] **KRIVADE Agnese,** *EU's video game sector must be more acknowledged and better funded,* 03/10/2022, Presse du Parlement européen, disponible sur https://www.europarl.europa.eu/news/en/press-room/20221003IPR42122/eu-s-video-game-sector-must-be-more-acknowledged-and-better-funded : "C'est l'un des rares secteurs créatifs à avoir connu une croissance de son chiffre d'affaires pendant la crise du Covid-19. Environ 98 000 personnes en Europe étaient employées dans le secteur du jeu vidéo en 2020. Selon l'IFSE, l'industrie européenne du jeu vidéo, la moitié des Européens se considèrent comme des joueurs de jeux vidéo, dont près de la moitié sont des femmes, l'âge moyen d'un joueur de jeux vidéo en Europe étant de 31,3 ans"

[12] https://zevent.fr

l'événement caritatif ayant levé le plus d'argent sur Twitch[13]. Parmi les joueurs de jeux vidéo français, 32% ont le sentiment d'appartenir à une communauté. Ce sentiment est partagé par 47% des enfants[14].

Enfin, si le jeu vidéo est un marché de consommateurs, il est également un marché de professionnels. On constate ainsi une volonté croissante de l'Union européenne d'investir dans le jeu vidéo, tant via des financements de la production locale que pour le développement de l'e-sport sur notre continent[15]. L'Europe se place ainsi comme deuxième mondial en ce qui concerne les revenus du e-sport avec plus de 300 millions d'euros de revenus[16].

Le jeu vidéo est donc bien identifié comme élément économique et commence progressivement à s'installer comme élément culturel permettant la diffusion d'un *soft power* européen dont les valeurs seraient positives. Le Parlement européen a ainsi adopté, le 10 novembre dernier, une résolution dans laquelle il souligne le fort potentiel des jeux vidéo et du sport électronique pour promouvoir « *l'histoire, l'identité, le patrimoine, les valeurs et la diversité européens au moyen d'expériences immersives* », estimant qu'ils sont également susceptibles de contribuer au pouvoir d'influence de l'Union[17].

Malheureusement, malgré toutes les meilleures intentions de pouvoir en faire une industrie vertueuse, les élans de solidarité et d'union de la communauté des joueurs et des développeurs sont souvent parasités : les plateformes – réseaux sociaux, streaming, jeux vidéo) – sont aussi le lieu de prédilection de comportements bien moins nobles, dont certaines puissances étrangères tirent profit : haine en ligne, cyberharcèlement[18], menaces de mort et de viol, propos sexistes, racistes, homophobes, néonazis, ou faisant l'apologie du terrorisme ou confortant une propagande étrangère. Le jeu vidéo, en tant qu'il se développe de plus en plus comme un média en ligne, n'échappe ainsi pas à l'ingérence étrangère qui accable le reste du monde du numérique.

2. Une ingérence étrangère déjà bien en place dans la sphère de gravitation du jeu vidéo

[13] **TOUZANI Samir**, « Z Event : le téléthon du streaming sur Twitch récolte plus de 10 millions d'euros », Lesechos.fr, 12 septembre 2022, , disponible sur : https://www.lesechos.fr/tech-medias/hightech/z-event-le-telethon-du-streaming-sur-twitch-recolte-plus-de-10-millions-deuros-1787261

[14] *ibid, v. 7.*

[15] **ROCHEFORT** Mathilde, "L'UE veut explorer tout le potentiel du jeu vidéo", 5/10/2022, sur *siecledigital.fr*, disponible en ligne sur : https://siecledigital.fr/2022/10/05/europe-jeux-video-investissement/

[16] **Europe's Video Games Industry** / **European Games Developer Federation**, *"Video games – A force for good - Key Facts from 2021"*, publié en 2022, données Ipsos.

[17] **FARRENG** Laurence, "Rapport sur le sport électronique et les jeux vidéo", 10 novembre 2022, point 16 du rapport, disponible en ligne sur : https://www.europarl.europa.eu/doceo/document/A-9-2022-0244_FR.html

[18] **TENAGLIA Adélaïde**, *Harcèlement sur Twitch : "Je reçois des messages néonazis, des photos de cadavres"*, publié le 26 janvier 2022, Télérama [EN LIGNE] : https://www.telerama.fr/ecrans/harcelement-sur-twitch-je-recois-des-messages-neonazis-des-photos-de-cadavres-7008438.php

En développement depuis plusieurs années, et plus particulièrement depuis le début de la guerre en Ukraine, les exemples concrets de désinformation, haine en ligne ou tentatives de déstabilisation de la démocratie à la faveur d'une puissance étrangère (bien souvent la Russie pour ne pas la nommer) se multiplient sur les réseaux sociaux et dans les médias.

[2.1. Des exemples concrets fréquents et préoccupants]

Beaucoup de ces exemples concernent notamment le groupe Wagner – société militaire privée russe Wagner Group dont le fondateur, Evgueni Prigojine, est proche de Vladimir Poutine – sont plus inquiétants les uns que les autres :

- Dans un rapport publié le 1er décembre 2022[19], la start-up américaine *NewsGuard* - créée en 2018 dans le contexte de l'explosion du flux de fake news partagée sur les réseaux sociaux, notamment lors des élections présidentielles de 2016 – constate que 160 vidéos sur *TikTok*, le réseau social chinois, glorifient des actes de violences perpétrées par le groupe Wagner, la société militaire privée menée par l'oligarque russe proche du président russe Vladimir Poutine, Evgueni Prigojine. Parmi ces vidéos, plus d'une dizaine semble montrer des extraits de l'exécution de Yevgeny Nuzhin, l'ancien mercenaire russe du groupe Wagner ayant décidé de rejoindre le camp ukrainien, survenue le 12 novembre 2022. Ces vidéos sont visibles dans leur intégralité sur *Telegram*, une messagerie instantanée dont la modération des contenus illicites est communément connue pour être hasardeuse, mais aussi sur le réseau *VKontakte*, le "Facebook russe"[20].
- Sur un canal Telegram pro-Kremlin, une vidéo a été diffusée dans laquelle un étui d'instrument de musique est remis, selon Evgueni Prigojine, patron de Wagner, au Parlement européen. Dans cet étui, une masse sur laquelle est gravé en cyrillique "PMC Wagner" et dont le manche porte des traces de sang. Bien que le colis ne soit en réalité jamais arrivé à destination (ni à Strasbourg, ni à Bruxelles)[21],cette démonstration a été diffusée dans plusieurs médias et sur plusieurs réseaux sociaux.
- Trois vidéos *TikTok* pro-Wagner publiées en novembre 2022 comportaient une URL redirigeant les internautes vers une chaîne *Telegram* du groupe Wagner sur laquelle il était diffusé des avis de recrutement, ainsi que les numéros de téléphone des recruteurs locaux du groupe Wagner dans 33 régions russes[22].

---

[19] v. site de NewsGuard : https://www.newsguardtech.com/fr/misinformation-monitor/novembre-2022/

[20] **SIX** Nicolas, "Sur TikTok, des vidéos de propagande pour le groupe paramilitaire Wagner", 01/12/2022, sur *Lemonde.fr*, disponible en ligne sur : https://www.lemonde.fr/pixels/article/2022/12/01/sur-tiktok-des-videos-de-propagande-pour-le-groupe-paramilitaire-wagner_6152459_4408996.html#xtor=AL-32280270-%5Bdefault%5D-%5Bandroid%5D

[21] **HORN** Alexandre, "Le patron de Wagner, Evgueni Prigojine, a-t-il envoyé une masse ensanglantée au Parlement européen ?", 24/11/2022, sur *liberation.fr*, disponible en ligne sur : https://www.liberation.fr/checknews/le-patron-de-wagner-evgueni-prigojine-a-t-il-envoye-une-masse-ensanglantee-au-parlement-europeen-20221124_TD6ZGH7FNZF2NFZPPYIZILXQ3U/

[22] ibid, point 18.

Si l'implication de la Russie dans des démonstrations d'intimidation des puissances occidentales s'est accentuée depuis le début de la guerre en Ukraine, cette stratégie de déstabilisation des processus démocratiques n'est cependant pas une première. Elle a notamment pu être constatée, et documentée, en amont du vote qui a conduit le Royaume-Uni à quitter l'Union européenne, mais également au moment de l'élection de Donald Trump comme président des Etats-Unis.

[2.2. L'ingérence systémique de la Russies dans les processus démocratiques européens]

Ainsi, dans son livre *Toxic Data : Comment les réseaux manipulent nos opinions,* David Chavalarias donne quelques exemples des moyens mis en œuvre par la Russie pour déstabiliser les systèmes politiques des États occidentaux. En outre, en 2021, le journal britannique *The Guardian* publie un ensemble de documents classés secrets par le Kremlin. Un compte rendu souligne l'intention russe *« d'influencer les systèmes politiques des gouvernements qui jouent un rôle central dans l'instauration ou l'élargissement des sanctions [contre la Russie après son invasion de la Crimée en 2014]* », notamment en provoquant « *l'apparition d'une crise socio-politique aux États-Unis »*[23]. Cette stratégie d'influence se décline dans trois espaces :

- Dans le processus électoral : le but était de faciliter la candidature du républicain Donald Trump à la présidence des États-Unis, notamment en raison des critiques que ce dernier avait à l'égard de l'OTAN ;
- Dans l'espace médiatique : cette stratégie reposait sur l'instauration d'un climat antisystème et d'une défiance collective envers les médias *via* des "virus médiatiques" ;
- Dans l'espace numérique : de nombreuses cyberattaques ont été réalisées, notamment celle du Comité national démocrate dans le but de divulguer des courriels internes et discréditer le camp démocrate.

Le lanceur d'alerte Christopher Wylie, ancien directeur de *Cambridge Analytica*, décrit dans son livre *Mindf*ck*[24] ces mêmes phénomènes. Il y dépeint également l'implication de la société *Cambridge Analytica* qui a fourni des données à des oligarques russes pour contribuer, grâce à ses algorithmes et ses méthodes de ciblage numérique, à la campagne du Brexit menée par Leave.EU. Cette stratégie a concrètement participé à précipiter la sortie du Royaume-Uni de l'UE.

Cette guerre de l'information tend à discréditer les gouvernements en place et les médias considérés comme "mainstream". Cette méthode est de plus en plus utilisée par les mouvance d'extrême droite, lors de lynchage en ligne, comme le met en évidence le journaliste Paul Conge dans son livre *Les grands-remplacés* : on constate une croissante défiance envers les médias traditionnels, mais aussi le développement progressif de médias qu'on pourrait qualifier qui se prétendent

[23] **CHAVALARIAS David**, *TOXIC DATA, "Comment les réseaux manipulent nos opinions", Chapitre 8 : "Diviser pour mieux régner depuis l'étranger"*, Mars 2022, Ed. Flammarion

[24] **WYLIE Christopher**, *Mindf*ck*, Mars 2020, Ed. Grasset, Chapitres 8 (pour les États-Unis) et 9 (pour le Royaume-Uni).

"alternatifs". En France, parmi ces médias alternatifs, il y a RT et Sputnik, des chaînes de télévision d'information internationale en continu financées par l'État russe.

L'usage des médias n'est qu'un élément parmi un ensemble de stratégies développées par les États étrangers pour s'ingérer dans nos processus démocratiques. Les fermes à trolls se révèlent en être un autre. Une ferme à trolls ou une usine à trolls est une organisation visant à coordonner des actions de *trolling* ou de *hacking*, via la diffusion massive d'informations mensongères ou partiels sur les réseaux sociaux, via des fausses identités, dans le but de de créer une pression ou une déstabilisation politique. Ce terme émerge dans la presse en 2015, lorsque des journalistes révèlent l'existence de l'entreprise *Internet Research Agency*, une entreprise de 300 personnes établie à Saint-Pétersbourg et dirigée par Evgueni Prigojine, un nom qui ne cesse de revenir dès qu'on parle d'ingérence russe. Cette « usine » a produit un ensemble de campagnes faisant l'éloge de Vladimir Poutine, notamment dans le contexte de l'annexion de la Crimée et de l'élection présidentielle américaine de 2020. Lyudmila Svachuk, une journaliste russe qui a réussi à infiltrer l'entreprise, alerte dès 2018[25] sur le fait qu'il n'y a *« aucun doute que les élections européennes seront fortement ciblées. Le but du Kremlin est toujours le même : créer du chaos pour ensuite essayer d'en tirer profit. L'Europe doit absolument muscler ses mécaniques de défense »*. Dans le contexte plus récent de la Guerre en Ukraine, les fermes à trolls ont été à nouveau utilisées : un rapport présenté par le gouvernement britannique souligne cette méthode manipuler l'opinion publique internationale pour diffuser la propagande pro-Kremlin[26].

3. Le jeu vidéo comme intermédiaire des réseaux d'ingérence

A ce stade, il nécessaire de rappeler que lorsqu'on mentionne le « jeu vidéo » il convient de garder en tête qu'il est fait référence à l'ensemble des dispositifs qui gravitent autour du jeu vidéo, à savoir le streaming, les forum, les plateformes vidéo, les tchats internes au jeu vidéo ainsi que les messageries.

Et à cet égard, le jeu vidéo est utilisé comme un intermédiaire visant à encourager les joueurs à aller sur des sites de propagande, des forums ou des discussions sur Discord ou Telegram relayant des idéologies illibérales. On va même jusqu'à constater un détournement du jeu vidéo à des fins terroristes. En ce sens, Gilles de Kerchove, le coordinateur de l'Union européenne pour la lutte contre le terrorisme, alerte sur la « sous-régulation » des jeux en ligne, identifiés comme un moyen alternatif de diffusion d'idéologies, en particulier de l'extrême droite[27].

---

[25] **PERROTE** Derek, "Visite guidée d'une « ferme à trolls » russe", 17 octobre 2018, *Lesechos.fr*, disponible en ligne sur : https://www.lesechos.fr/tech-medias/hightech/visite-guidee-dune-ferme-a-trolls-russe-142088

[26] **AFP**, "Russie : une "usine à trolls" comme arme dans la guerre de l'information", le 27 avril 2015, sur *lexpress.fr*, disponible en ligne sur : https://www.lexpress.fr/monde/video-russie-une-usine-a-trolls-comme-arme-dans-la-guerre-de-l-information_1675231.html

[27] **AFP**, "Les jeux en ligne "sous-régulés", pour le coordinateur de l'antiterrorisme de l'UE", dans *lexpress.fr*, 26/11/2020, disponible en ligne sur :

Dans l'ensemble ses travaux, Paul Conge a enquêté sur une nouvelle génération de militants qui déploient là où on aurait pu le moins s'y attendre en politique : le jeu vidéo. Le journaliste a infiltré une mouvance négationniste qui recrute des jeunes joueurs sur le jeu gratuit *Fortnite Battle Royal*, un jeu de tir à la troisième personne[28]. Grâce à ces méthodes, le groupuscule parvient à recruter nombreux de jeunes joueurs qui sont ensuite redirigés vers les messageries extérieures au jeu, telles que Discord. Sur ces messageries, ils proposent alors des actions militantes appelées "irl" (*in real life*, en français : « dans la vraie vie »), des "raids numériques", consistant par exemple à des activités de cyberharcèlement massif, ou encore de "l'*astroturfing* numérique", une technique consistant à simuler un mouvement spontanée de l'opinion public en hissant artificiellement des tweets ou des hashtags en tendance sur Twitter. Ce type de mouvances ciblent des joueurs jeunes, souvent isolés socialement, et donc plus réceptifs aux théories complotistes et plus faciles à radicaliser. Ces méthodes sont en réalité les mêmes que celles utilisées par les États étrangers pour influencer l'opinion public en Europe, d'autant que le lien entre extrême-droites européennes et influence du Kremlin se fait de plus en prégnant, ainsi que le démontre Chloé Ridel dans son ouvrage *D'une guerre à l'autre*[29].

Enfin, le jeu vidéo, lorsqu'il est produit et développé à l'étranger, est un *soft power* de nature à influencer directement les consommateurs de jeu en Europe. Il est alors directement utilisé comme méthode de diffusion des idées illibérales, par le biais de la *gamification* des discours haineux, constituant ainsi un dernier outil pertinent pour la transmission d'idéologie. On entend par *gamification* l'utilisation des mécaniques de jeu dans un contexte extérieur au jeu. En d'autres termes, il s'agit là de l'utilisation de techniques spécifiques aux jeux vidéo pour fidéliser et engager les utilisateurs. Les mécanismes de gamification sont désormais quotidiens : points, niveaux, récompenses, statut (« argent », « gold », « platinum »), carte de fidélité, etc. Appliqué au jeu vidéo, ce phénomène de gamification des discours haineux et idéologiques s'exprime notamment par le biais de jeux vidéo tels que celui reprenant l'ensemble des codes suprémacistes blancs et néo-nazis dans lequel il est possible d'incarner Adolf Hitler, Jair Bolsonaro, Vladimir Poutine, ou encore Breton Tarrant, le terroriste d'extrême droite auteur de l'attentat de Christchurch[30].

L'analyse combinée du nombre de joueurs concernés par le monde du jeu vidéo et de l'étendue du phénomène d'ingérence étrangère par les moyens numériques démontre ainsi le niveau d'exposition - et donc de vulnérabilité - de ce secteur. La question naturelle qui se pose alors est celle de savoir comment il est protégé et réglementé - et malheureusement, il apparaît, en y regardant de plus près, que les outils réglementaires à disposition, bien qu'existants, ne sont pas des plus adaptés.

---

https://www.lexpress.fr/monde/les-jeux-en-ligne-sont-sous-regules-pour-le-coordinateur-de-l-antiterrorisme-de-l-ue_2139479.html

[28] **COUSSEAU Cédric**, "J'ai infiltré une mouvance d'extrême-droite qui recrute des jeunes sur Fortnite", 8 septembre 2020, sur *francetvinfo.fr*, disponible en ligne sur : https://www.francetvinfo.fr/economie/emploi/metiers/video-j-ai-infiltre-une-mouvance-d-extreme-droite-qui-recrute-des-jeunes-sur-fortnite_4093461.html

[29] **RIDEL** Chloé, *D'une guerre à l'autre: l'Europe face à son destin*, 25/08/2022

[30] **MACÉ Maxime, PLOTTU Pierre,** "Ces jeux vidéo dont les racistes sont les héros", 19/11/2020, sur Slate.fr, disponible en ligne sur : https://www.slate.fr/story/197205/jeux-video-heros-raciste-gamification-extreme-droite-propagande-radicalisation

PARTIE II : UNE RÉGLEMENTATION PARCELLAIRE AUTOUR DES PRATIQUES LIÉES AUX JEUX VIDÉOS

Le jeu vidéo est un outil auquel les décideurs politiques en général, et les législateurs en particulier, s'intéressent relativement peu. Longtemps considéré comme un bien économique comme un autre, le jeu vidéo est un bien de plus en plus exposé politiquement, du fait de son développement autour de l'interaction entre joueurs en ligne, ainsi qu'on l'a vu précédemment. S'il ne s'agit évidemment pas d'empêcher la liberté d'expression qui doit avoir cours sur ce type de plateformes, il convient néanmoins de pouvoir être en mesure d'en sanctionner les abus, surtout s'il mène à la prolifération de contenus à caractère haineux, manipulatoires ou de la désinformation, instrumentalisée par des puissances étrangères.

Si, à cet égard, on peut tenter d'utiliser la réglementation européenne récemment adoptée en matière de contenu en ligne (A.), force est de constater que le jeu vidéo continu de rester, à tort, en dehors du cadre des réflexions actuelles relatives à la protection contre l'ingérence étrangère, notamment depuis le début de la guerre en Ukraine (B.).

1. Une législation numérique longuement attendue mais sans mention du jeu vidéo

[1.1. La stratégie numérique de l'UE]

Les institutions européennes développent souvent des stratégies politiques dès lors qu'elles constatent leur retard dans un domaine. C'est le cas pour le numérique, dont la planification stratégique n'a commencé qu'en 2010. Entre 2010 et 2020, l'Union européenne a développé une première stratégie numérique. Le bilan de cette période a permis le développement d'une meilleure connectivité pour tous les Européens, mais aussi d'assurer une meilleure protection des utilisateurs concernant leur vie privée[31] et leurs données[32]. Depuis 2020, et jusqu'en 2030, les enjeux de la cybersécurité sont croissants. L'Union développe une nouvelle stratégie axée sur la nécessité de développer des marchés et des services sûrs et sécurisés. L'essentiel des réglementations se concentrent sur la protection des infrastructures du cyberespace (résilience face aux cyberattaques, élaborer d'infrastructures plus performantes), mais aussi à protéger l'ensemble des éléments de la couche informationnelle du cyber (informations, utilisation de l'intelligence artificielle pour traiter les données, etc.). Pour autant, dans un environnement où le développement numérique est plus rapide que le temps du politique et du droit, les normes sont donc élaborées en réaction plutôt que par anticipation aux enjeux numériques. Les enjeux de la cybersécurité sont croissants.

[31] Directive 2009/136/CE
[32] Directive 95/46/CE

Le début de cette nouvelle stratégie décennale a été marquée par l'élaboration de deux principaux paquets numériques : le *Digital Markets Act* (aussi appelé « DMA »), qui réglemente les marchés numériques, et le *Digital services act* (« DSA »), qui constitue la législation européenne en matière de services numériques.

Le *Digital Markets Act* visant à assurer davantage de compétitivité sur le marché numérique et à garantir des comportements équitables en ligne entre les plateformes et les contrôleurs d'accès, mesures coercitives et sanctions à l'appui, ce règlement, qui entrera en application le 2 mars 2023, vise principalement à empêcher les abus de positions dominantes des géants du numérique pour offrir plus de choix aux consommateurs européens. Il ne concerne donc pas directement le jeu vidéo et ne sera donc pas analysée plus en détails dans le cadre de cette étude.

Le *Digital Services Act*, quant à lui, vise à lutter contre les contenus et produits illégaux en ligne, allant des contenus haineux, pédopornographiques et terroristes, à la désinformation, en passant par la contrefaçon, avec le mot d'ordre : *"ce qui est illégal hors ligne doit également être illégal en ligne"*. Il s'agit d'une modernisation d'une partie de la directive de 2000 sur le commerce électronique[33], dont l'objectif est de favoriser une utilisation plus sûre d'Internet. Il a commencé à entrer en vigueur le 16 novembre 2022 (pour les plateformes « les plus grandes ») et finira d'entrer en vigueur au plus tard en février 2024.

S'il apparaît évident que le jeu vidéo devrait respecter les dispositions du DSA, la mise en œuvre des obligations imposées par le règlement reste beaucoup plus incertaine. En effet, le DSA prévoit la responsabilité des contenus illicites relatives aux « plateformes ». Les principales visées sont les plateformes de réseaux sociaux ou les plateformes de commerce électronique.

[1.2. Le DSA et la responsabilité des contenus illicites]

En effet, la notion de responsabilité des contenus illicites sur les plateformes (réseaux sociaux, hébergeurs de contenus) suppose que les plateformes elles-mêmes ne sont pas responsables d'une vidéo, d'un texte ou d'un commentaire haineux postés par un utilisateurs, mais qu'elles en sont deviennent responsables si elles ont connaissance de leurs caractère illicite et qu'elles ne les retirent pas, endéans un certain délai.

Or, la diversité des définitions de la notion de contenus illicites ne permet pas une protection harmonisée et adaptée, tant pour les internautes que pour les plateformes. Ces dernières peinent en effet à identifier si elles doivent censurer ou non certains contenus, cherchant toujours l'équilibre entre liberté d'expression et protection de l'Internet, ce qui risque de créer une insécurité juridique certaine.

On suppose donc que les plateformes de vente de jeux vidéo en ligne sont également à qualifier de « plateformes » au sens du règlement européen, et que

[33] Directive 2000/31/CE

donc, une partie de la réalité du jeu vidéo est concernée par la réglementation. Mais quid de l'existence de tchats s'apparentant à des messageries instantanées ? à des réseaux sociaux ? L'ensemble du macrocosme informatique qui gravite autour du jeu vidéo ne peut donc que partiellement être intégré dans la notion de plateformes, et encore, selon une interprétation extensive de la réglementation. Et à la lecture du règlement, et des documents transmis aux institutions européennes en amont de son adoption[34], il apparaît clair que, d'une manière générale, le jeu vidéo n'était pas l'objet principal de la réglementation visée, et qu'elle n'est donc pas la plus adaptée à la réalité inhérente au jeu vidéo, encore moins aux problèmes d'ingérence dont il est victime.

[1.3. La difficulté de définir les contenus illicites haineux]

En outre, si le but est, en principe, de sanctionner les contenus illicites, le règlement ne définit pas lui-même ce qu'il faut entendre par là. On comprend bien ici que la volonté du législateur européen a été de laisser les Etats membres libres d'adapter la définition à leur contexte juridique national. Néanmoins, c'est à nouveau une incertitude supplémentaire quant à l'application – ou non – de sanctions relatives aux agissements répréhensibles sur les plateformes de jeu vidéo, et plus particulièrement en ce qui concerne la haine ou la désinformation.

En effet, il n'existe pas une définition consensuelle du discours haineux dans l'Union européenne[35]. Chaque État membre dispose de sa propre conception de la notion de discours haineux. À l'échelle de l'Union européenne, la notion juridique retenue est celle du contenu illicite, une notion bien plus large, qui permet, en principe, d'englober les discours haineux, mais aussi la désinformation ou l'apologie du terrorisme.

Il est intéressant à ce stade de noter que le discours de haine est un phénomène qualifié par le Conseil de l'Europe (qui, pour rappel n'est pas une institution de l'Union européenne) comme "enraciné, complexe et multidimensionnel". On entend par discours de haine "tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que la «race», la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle."[36] Le Comité des ministres insiste également sur le fait que la diffusion de ces discours haineux via internet – notamment au regard de

[34] Europe's Video Games Industry (ISFE), Position Paper on the Digital Services Act, May 2021, disponible en ligne sur: https://www.isfe.eu/wp-content/uploads/2021/05/ISFE-DSA-Position-Paper-May-2021.pdf

[35] **LEQUEUX Vincent**, *Haine en ligne : que fait l'Union européenne ?,* mis à jour le 03/02/2022, sur *Touteleurope.eu*, disponible en ligne sur : https://www.touteleurope.eu/economie-et-social/facebook-youtube-instagram-comment-l-europe-lutte-t-elle-contre-les-contenus-illicites-en-ligne/

[36] **Comité des Ministres du Conseil de l'Europe**, Recommandation CM/Rec(2022)16, adoptée le 20 mai 2022 lors de la 132e Session du Comité des Ministres, disponible en ligne : https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a67951

l'ubiquité d'internet, de son absence de territorialité et de son instantanéité – est d'autant plus dangereuse que le discours haineux y amplifie son impact, y compris hors ligne. Ces discours participent à la stigmatisation des personnes ciblées et découragent la participation au débat public, ce qui est préjudiciable à la démocratie.

Ainsi qu'il a été développé dans la première partie de cette étude, l'ingérence étrangère est un vecteur direct de la diffusion de la haine en ligne. Or, la diffusion de discours haineux via internet tend à toucher l'ensemble des internautes européens, d'où la nécessité d'être en mesure de réglementer les services numériques pour limiter la diffusion de ces contenus haineux de manière précise et efficace.

[1.4. La tentative de réglementation en matière de contenus haineux sur internet en France]

Au niveau français, il est intéressant de noter l'adoption de la Loi du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, dite loi « Avia »[37], en amont de l'adoption du DSA. Cette loi, qui avait pour but de renforcer la contribution des opérateurs numériques à la lutte contre certains contenus manifestement haineux en ligne a cependant fait l'objet d'une importante censure du Conseil constitutionnel.

À l'origine, la proposition de loi, telle qu'adoptée par le Parlement, obligeait les opérateurs de plateforme en ligne et les moteurs de recherche à retirer les contenus manifestement illicites tels que les incitations à la haine, les injures à caractère raciste ou anti-religieuses notifiés par une ou plusieurs personnes, dans un délai de 24 heures, ce délai étant réduit à une heure pour les contenus terroristes ou pédopornographiques.

Cependant, soucieux de l'équilibre entre sauvegarde de l'ordre public, d'une part, et liberté d'expression et de communication, d'autre part, le Conseil constitutionnel a censuré ces dispositions dans sa décision du 18 juin 2020, considérant que le législateur portait une atteinte à la liberté d'expression qui n'était ni adaptée, ni proportionnée au but poursuivi[38]. La censure de ces dispositions a pour conséquence la censure des dispositions du texte qui organisaient la mise en œuvre de l'obligation de retrait de contenus.

Cette loi n'a donc plus d'intérêt qu'en ce qu'elle crée un observatoire de la haine en ligne, placé sous le contrôle du Conseil supérieur de l'audiovisuel (CSA) et chargé du suivi et de l'analyse de l'évolution des contenus haineux, en lien avec les opérateurs, associations et chercheurs concernés.

Les réseaux sociaux ont été identifiés comme un intermédiaire privilégié de diffusion de contenus considérés comme illicites, en ce compris les discours de haine, dont il a été démontré précédemment qu'ils sont encouragés par certaines puissances étrangères. Cependant, alors même que les nouvelles dispositions de régulation attendent encore de

[37] Loi n°2020-766 adoptée le 24 juin 2020, dite loi Avia, contre les contenus haineux sur internet
[38] Conseil constitutionnel, décision n°2020-801 DC du 18 juin 2020

pouvoir entrer en vigueur, on constate qu'elles sont déjà inadaptées aux réalités de terrain que représente le monde du jeu vidéo.

Pourtant, il apparaît évident que les institutions politiques, notamment européennes, entendent faire évoluer le cadre réglementaire rapidement pour lutter contre ingérence politique et désinformation. Néanmoins, il semble que le jeu vidéo fasse figure de grand oublié des réflexions menées, qui vont pourtant dans le bon sens.

2. Ingérence étrangère et jeu vidéo : une prise de conscience européenne en silos

L'Union européenne, lors des évènements relatifs à la guerre en Ukraine et aux cyberattaques, a brillé par sa réactivité[39], exemple que si la réponse politique doit être rapide, il est parfois possible d'agir rapidement. Concernant les propositions réglementaires liées au jeu vidéo, elles continuent également de se développer, mais sur une trajectoire qui semble être parallèle à celle qui se construit autour de l'ingérence : jusqu'ici, elles ne sont pas destinées à se croiser, voire à évoluer conjointement, ce qui est regrettable dans un contexte dans lequel il est démontré l'utilisation du jeu vidéo comme outil d'ingérence.

[2.1. Sur l'ingérence et la cybersécurité]

Les différentes tentatives d'ingérence étrangère s'incarnent par le biais de canaux aussi divers que variés, au premier rang desquels se place le numérique. *« Il n'y a pas d'Europe de la défense sans une Europe de la cyberdéfense »* a déclaré Margrethe Vestager, commissaire à la Direction générale de la concurrence de la Commission européenne, lors du récent débat sur la proposition de directive relative à la réforme de l'harmonisation de la cybersécurité dans l'Union européenne (NIS2[40]). Ces mots prennent tout leur sens lorsque le Parlement européen, quelques semaines plus tard,

[39] **OMNES** Ophélie, **VERDIER** Théo, *Guerre en Ukraine : Analyse de la réponse européenne*, 23 mars 2022, Fondation Jean-Jaurès, disponible en ligne sur : https://www.jean-jaures.org/publication/guerre-en-ukraine-analyse-de-la-reponse-europeenne/

[40] **GROOTHUIS Bart**, Rapport sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union [NIS2], abrogeant la directive (UE) 2016/1148 [NIS] : HYPERLINK "https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738184/EPRS_ATA(2022)738184_FR.pdf"https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738184/EPRS_ATA(2022)738184_FR.pdf

après avoir adopté une résolution[41] reconnaissant la fédération de Russie en tant qu'État soutenant le terrorisme[42], est visé par une cyberattaque imputée à des pirates russes[43].

[2.1.1. La prise de conscience des enjeux relatifs à l'ingérence lors du déclenchement Guerre en Ukraine]

Au lendemain de l'invasion russe en Ukraine, les parlementaires européens ont partagés leurs inquiétudes et leurs préoccupations concernant *« l'incidence croissante et la nature de plus en plus sophistiquée des tentatives d'ingérence et de manipulation de l'information étrangères, essentiellement menées par la Russie et la Chine et visant tous les aspects du fonctionnement démocratique de l'Union européenne et de ses États membres »*[44]. En effet, dans un rapport adopté, relatif à l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union, y compris la désinformation[45], les eurodéputés ont appelé au renforcement des infrastructures critiques et stratégiques et secteurs stratégiques, mais aussi sur les réseaux-sociaux par le phénomène de la désinformation.

Cette prise de conscience du Parlement européen de l'utilisation du numérique grand public pour des phénomènes d'ingérence étrangère intervient à retardement. D'autre part, les enquêtes de la presse, qui mettaient jusque-là en évidence des phénomènes d'ingérence *via* les réseaux sociaux, alertent désormais sur l'émergence d'une propagande pro-russe et autres mouvances d'extrême-droite sur les réseaux sociaux[46]. Or, les jeux vidéo n'ont pas été mentionnés dans le rapport du Parlement européen, et le jeu vidéo ou le domaine du divertissement numérique n'est pas mentionné dans les propositions d'extensions des infrastructures critiques et stratégiques proposées par le Parlement.

---

[41] **ALMQVIST Viktor, KOBEŠĆAK SMODIŠ Snježana**, "Le Parlement européen déclare que la Russie est un État soutenant le terrorisme, communiqué de presse du Parlement européen", 23 novembre 2022, https://www.europarl.europa.eu/news/fr/press-room/20221118IPR55707/le-parlement-europeen-declare-que-la-russie-est-un-etat-soutenant-le-terrorisme

[42] Proposition commune de résolution (Renew, PPE, ECR, (2022/2896(RSP)) - adoptée avec une large majorité, 494 voix pour, 58 contre, 44 abstentions. Disponible en ligne sur : https://www.europarl.europa.eu/doceo/document/B-9-2022-0482_EN.html

[43] **Contexte**, Briefing du 24 novembre 2022, sur *contexte.com* disponible en ligne sur : https://www.contexte.com/actualite/pouvoirs/le-parlement-europeen-vise-par-une-cyberattaque-imputee-a-des-pirates-russes-apres-le-vote-dune-resolution-anti-moscou_159762.html

[44] **KALNIETE Sandra**, Rapport sur *l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation*, résolution adoptée par le Parlement européen le 9 mars 2022 : https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_FR.html ; citation extraite du rapport, point 1, sur la Nécessité d'une stratégie coordonnée de l'Union contre l'ingérence étrangère.

[45] *ibid.*

[46] **COUSSEAU Cédric**, Guerre en Ukraine : comment la propagande prorusse tente d'infiltrer les jeux vidéo, YouTube et Facebook, le 4 mars 2022, Franceinfo.fr, [EN LIGNE], https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-comment-la-propagande-prorusse-tente-d-infiltrer-des-canaux-de-diffusion-comme-wikipedia-et-les-jeux-video_4989436.html

[2.1.2. La considération croissante des enjeux de la cybersécurité]

Les enjeux du numérique et de la cybersécurité constituent un intérêt croissant pour l'Union, comme en témoigne l'actualisation de la première directive sur la sécurité des réseaux et des systèmes d'information (aussi appelée SRI, ou NIS). Cette première directive de l'Union sur la cybersécurité a en effet été perfectionnée à l'automne 2022 avec la proposition de directive NIS2 / SRI2[47], adoptée en plénière le 10 novembre 2022. La proposition est désormais entre les mains du Conseil, dans l'attente de son adoption.

S'il est évident que cette directive participera activement à renforcer l'architecture juridique et opérationnelle de l'Union en matière de cybersécurité, les enjeux relatifs à la protection du secteur du divertissement contre les cyberattaques criminelles ne sont pas mentionnés. Par conséquent, le jeu vidéo est également le grand absent de cette réforme du numérique, bien qu'il soit un enjeu de taille pour la cybersécurité européenne et pour les citoyens européens.

[2.2. Le jeu vidéo, un objet du droit de l'Union]

Le jeu vidéo apparaît comme un « objet juridique non identifié » pour l'Union européenne : il est difficile de le définir, mais également d'identifier les enjeux politiques qui lui sont consacrés – sont-ils économiques ? culturels ? sociaux ? Les réglementations relatives au *res numericus* touchent en effet à l'ensemble des domaines du cyber. Elles touchent notamment aux enjeux de protection des données, de protection du consommateur et du marché intérieur. Le jeu vidéo ne semble jamais être identifié comme l'objet principal d'une réglementation ; il est toujours considéré de manière subsidiaire, quand il l'est. De plus, il est majoritairement considéré comme un objet économique sur un marché de consommateurs.

[2.2.1. Quelle approche dans la production législative ?]

Fidèle à l'ancienne stratégie décennale, la réglementation du jeu vidéo et les consoles, comme l'ensemble des produits électroniques, sont soumis à la Réglementation générale pour la protection des données (RGPD). Cette protection est d'autant plus renforcée au regard du large public des jeux de moins de 18 ans. L'utilisation des données est une préoccupation croissante, d'autant plus que les systèmes basés sur l'intelligence artificielle prolifèrent dans le secteur du jeu vidéo. Ces systèmes influencent directement la manière dont nous consommons des produits, des services et des contenus : l'intelligence artificielle et les données permettent d'élaborer des stratégies de monétisation et de diffusion ciblées, y compris la diffusion de contenus haineux ou issus d'une ingérence étrangère.

[47] **GROOTHUIS Bart**, Rapport sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union [NIS2], abrogeant la directive (UE) 2016/1148 [NIS] : https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738184/EPRS_ATA(2022)738184_FR.pdf

L'utilisation des données, publiques comme privées, est un enjeu croissant dans les questions relatives à la cyberdéfense, notamment en raison de l'utilisation abusive et détournée de ces données par les puissances étrangères à des fins politiques ou commerciales. Sur le plan économique mais aussi financier, le jeu vidéo est fortement impacté par l'avènement des crypto-actifs, les NFT et autres nouveaux modèles de monétisation. Le jeu vidéo est au cœur d'une économie physique et numérique, notamment en raison de la multiplication des plateformes de vente virtuelle (telles que Steam, Playstation store, Nintendo Store, etc.).

[2.2.2. Quelle approche dans les derniers rapports des commissions du Parlement européen ?]

Le jeu vidéo est généralement considéré comme un pur objet économique. Plus récemment, le jeu vidéo est enfin reconnu, et à juste titre, comme un objet culturel. La dernière résolution du Parlement européen intitulée *Sport électronique et jeux vidéo*[48] illustre cette nouvelle tendance. Ce rapport a été saisi au fond par la commission CULT (culture et éducation), et pour avis par la commission IMCO (marché intérieur et protection des consommateurs). Dans ce rapport, et pour la première fois, le jeu vidéo est reconnu comme un élément de *soft power* européen.

Parallèlement à cette résolution, l'espagnole Adriana MALDONADO LÓPEZ (S&D), membre de la commission IMCO, a préparé un rapport d'initiative adopté en commission le 12 décembre 2022, dernier relatif à la protection des consommateurs dans les jeux vidéo en ligne[49]. Un vote en plénière est, à ce jour, prévu pour le 16 janvier 2023. Ce nouveau rapport souligne l'absence d'approche unique et coordonnée. La commission parlementaire cherche ainsi à trouver *« un équilibre entre la contribution du secteur des jeux en ligne au développement des technologies numériques et la nécessité d'évaluer son impact social, culturel et économique* ».

Ces deux rapports soulignent l'intérêt croissant de l'Union pour cet objet de divertissement et pour une compréhension plus large qu'en tant que simple objet de consommation. S'il est encourageant de constater cette ouverture, il reste regrettable qu'aucune commission n'ait saisi le sujet de l'ingérence étrangère dans ce secteur.

À ce jour, il n'existe donc aucun rapport entre les mains des commissions INGE2 (ingérence étrangère, y compris dans nos processus démocratiques) ou AFET (affaires étrangères) qui traite directement ou indirectement, ou qui mentionne, le jeu vidéo. Il reste encore difficile pour les décideurs politiques d'appréhender une toute autre dimension du jeu vidéo, notamment dans une conception plus sociale, politique ou stratégique.

Le jeu vidéo est un outil de diffusion de haine en ligne, et de désinformation, et par là-même, un outil d'ingérence étrangère. Pour autant, la réglementation en vigueur, et les projets de

[48] Sport électronique et les jeux vidéo, 10 novembre 2022, disponible en ligne sur : https://www.europarl.europa.eu/doceo/document/TA-9-2022-0388_FR.html

[49] MALDONADO LÓPEZ Adriana (S&D), Consumer protection in online video games: a European Single Market approach, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/2014(INI)

réglementations en cours, ne permettent pas encore une réponse à la hauteur de l'enjeu constaté. Si on constate progressivement une prise de conscience salutaire au niveau des institutions européennes, menant au début de la riposte, force est de constater qu'à ce stade, le jeu vidéo ne semble encore par avoir été intégré à cette réflexion pourtant globale. Devant l'urgence et l'importance de la question, comment faire en sorte de protéger efficacement ce macrocosme complexe ?

PARTIE III : LES MOYENS D'ACTION À ENVISAGER POUR LA RIPOSTE

Pour faire face à la menace que représente l'ingérence étrangère sur les Européens, au plus près de chez eux, par le biais des jeux vidéo, la réponse politique est indispensable mais pas suffisante.

En effet, s'il est essentiel que les institutions, nationales comme européennes, soient en mesure d'apporter une réponse efficace contre les tentatives de déstabilisation de la démocratie en Europe (1.), la protection du monde du jeu vidéo, raison de sa nature protéiforme, doit passer par l'implication de tous les acteurs concernés, au premier rang desquels se trouvent les communautés de joueurs (2.), figures d'autorité de fait, mais également les joueurs eux-mêmes, grâce à une pédagogie qu'il faut développer dès le plus jeune âge (3.).

Ces quelques éléments ne sont bien sûr que des pistes de réflexions destinées à ouvrir un débat public nécessaire autour de la question des différentes implications du jeu vidéo, et n'ont donc pas vocation à être exhaustives.

1. Le plaidoyer à destination des institutions nationales et européennes

Alors que le Parlement européen est en proie à un scandale dans le cadre d'une enquête en Belgique sur des soupçons de corruption au profit du Qatar, dans laquelle quatre personnes, dont une des vice-présidentes du Parlement européen, Eva Kaili, ont été écrouées, il est urgent de questionner la manière dont l'Union européenne souhaite envisager sa riposte contre les multiples atteintes à son intégrité venues de l'étranger, comment elle veut la mettre en œuvre.

Au moins où cette étude est rédigée, les premières réactions des institutions politiques de l'Union ont déjà manifesté leur indignation face à ce nouveau scandale, on constate, comme c'est (trop) souvent le cas en matière d'ingérence étrangère, mais également en matière numérique, que l'Union agit souvent en réaction plus qu'en anticipation. Heureusement, lorsque la volonté politique y est, les choses peuvent aller très vite, comme on a pu le constater avec la réponse européenne à la guerre en Ukraine[50].

Concernant le jeu vidéo plus particulièrement, il est essentiel à ce stade, qu'il puisse enfin être considéré par les institutions, nationales comme européennes, comme l'objet complexe qu'il est : à savoir un bien économique, mais aussi un bien culturel, qui a donc

[50] **OMNES** Ophélie, **VERDIER** Théo, *Guerre en Ukraine : Analyse de la réponse européenne*, 23 mars 2022, Fondation Jean-Jaurès, disponible en ligne sur : https://www.jean-jaures.org/publication/guerre-en-ukraine-analyse-de-la-reponse-europeenne/

nécessairement pour conséquence d'en faire un objet politique, tels quels le sont également les réseaux sociaux, comme le précise Nicolas Arpagian, spécialiste en cybersécurité : *« Il y a quelques mois un certain nombre de décideurs ignoraient tout de TikTok. C'est maintenant un lieu d'épanouissement, d'échange. Pareil pour Twitch, qui était réservé aux amateurs de jeux vidéo et qui est devenu un lieu d'expression politique. »*[51]

On pourra ainsi recommander plusieurs types d'action :

[1.1. Développer des mécanismes de contrôle, de veille et de protection]

- Renforcer les outils juridiques contraignants disponibles et les appliquer en matière de jeu vidéo

Ainsi qu'il a été démontré précédemment, l'Union européenne se dote progressivement d'un arsenal législatif ambitieux en matière de numérique, et progressivement en matière de lutte contre l'ingérence étrangère. Néanmoins aucune mention n'est jamais faite dans ce secteur concernant le jeu vidéo. Si une révision du DSA semble bien peu réaliste, alors que le texte attend encore de pouvoir entrer pleinement en vigueur, il n'est cependant pas encore trop tard pour faire entre les infrastructures liées aux jeux vidéo dans le champ d'application du NIS2.[52,53]

- Encourager le développement d'outils pour la régulation du contenu en ligne, tels que PHAROS et *Viginum*, au niveau européen :

    - PHAROS (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) est une plateforme créée le 16 juin 2009 par le Gouvernement français pour signaler des contenus et comportements en ligne illicites. Elle intègre l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une branche de la direction centrale de la Police judiciaire.

  Si elle permet de signaler des faits de pédophilie et pédopornographie, expression du racisme, de l'antisémitisme et de la xénophobie, incitation à la

[51] **MATHEVON** Franck, *Viginum, l'agence gouvernementale qui lutte contre les ingérences numériques étrangères entre en piste,* 15 octobre 2021 : https://www.radiofrance.fr/franceinter/viginum-l-agence-gouvernementale-qui-lutte-contre-les-ingerences-numeriques-etrangeres-entre-en-piste-1780820

[52] **GROOTHUIS Bart**, Rapport sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union [NIS2], abrogeant la directive (UE) 2016/1148 [NIS] : https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/738184/EPRS_ATA(2022)738184_FR.pdf

[53] voir en ce sens le 2.1.2. de cette étude, "La considération croissante des enjeux de la cybersécurité".

haine raciale, ethnique et religieuse et d' escroquerie et arnaque financières utilisant internet, elle est surtout active et performante en matière de terrorisme et apologie du terrorisme[54].

- *Viginum*[55] : il s'agit d'un service technique et opérationnel de l'État français, rattaché au Premier ministre et placé auprès du secrétaire général de la Défense et de la Sécurité nationale, chargé d'identifier les opérations impliquant directement ou indirectement des États étrangers, et plus précisément protection la France contre les ingérences numériques étrangères.

Par exemple, le camp russe, et plus précisément la « galaxie Prigojine » a interféré dans les campagnes présidentielle et législative de 2022 en France, en créant des faux comptes pro ou anti-électoral depuis le Mali, le Sénégal, le Bénin et la République Centrafricaine. En France, durant la période électorale de 2022, une soixantaine de phénomènes qualifiés d'"inauthentiques" sur les plateformes numériques ont été recensés par *Viginum*.

Au niveau européen, il existe bien une *East StratCom task force*, une organisation participant au service européen pour l'action extérieure et chargée d'assurer la promotion des activités de l'Union en Europe de l'Est (y compris au-delà des frontières communautaires). Elle est chargée de traquer les campagnes de désinformation et de propagande, spécifiquement russe, démontrant ainsi que l'Union européenne assume sa préoccupation contre l'ingérence russe, plutôt que l'ingérence chinoise, contrairement aux États-Unis. À ce jour, *East StratCom task force* n'a cependant pas traité de questions relatives à l'ingérence étrangère dans le jeu vidéo, et il serait nécessaire d'élargir le champ d'action d'une telle taskforce, puisque l'Europe de l'Est est loin d'être le seul territoire à risque dans l'Union européenne.

[1.2. Encourager les mécanismes visant à renforcer les outils de soft law (et prendre compte les limites inhérentes) tels que les code de conduite]

---

[54] **LECLÈRE** Emmanuel, "Pharos : 9.720 demandes de retrait de contenus internet à caractère terroriste depuis janvier", le 11/10/2021, sur *radiofrance.fr*, disponible en ligne sur : https://www.radiofrance.fr/franceinter/pharos-9-720-demandes-de-retrait-de-contenus-internet-a-caractere-terroriste-depuis-janvier-3870876

[55] **AFP**, "Ingérence en ligne : 60 cas douteux recensés lors des élections françaises de 2022", 25/10/2022, sur *lefigaro.fr*, disponible en ligne sur : https://www.lefigaro.fr/secteur/high-tech/ingerence-en-ligne-60-cas-douteux-recenses-lors-des-elections-francaises-de-2022-20221025

Exemples de *soft law* ayant porté leur fruits au niveau européen :

- En mai 2016, la Commission européenne, épaulée de plusieurs plateformes, a lancé le Code de conduite sur la lutte contre les discours haineux illégaux en ligne, qui a, depuis, fait l'objet d'évaluations successives ayant pour but d'améliorer l'outil.

  Son but : démontrer l'engagement des plateformes à *« faciliter la notification des discours haineux illégaux par leurs utilisateurs et à coopérer en ce sens avec les organisations de la société civile et les autorités nationales »*. Bien qu'il s'agisse d'un outil non contraignant, il faut souligner ici le volontarisme européen coordonné entre institutions et plateformes pour aboutir à un ensemble de règles respectées par le plus grand nombre.

- Suivant le même modèle, le Code de bonnes pratiques de 2022 en matière de désinformation[56] a été élaboré afin de répondre aux orientations formulées par la Commission européenne en la matière en 2021. Il résulte des travaux menés par les 34 signataires, qui ont adhéré au processus de révision du code 2018 et représentent un large éventail d'acteurs, tels que les plateformes en ligne, les acteurs de l'écosystème publicitaire, les vérificateurs de faits, la société civile, la recherche et d'autres organisations (parmi lesquels : Adobe, Microsoft, Twitter et Twitch).

Il convient de rappeler à ce stade que les outils précités ne sont pas contraignants et ne permettent que de donner un poids moral aux dispositions envisagées.

[1.3. L'approfondissement de la protection des mineurs est nécessaire mais pas suffisante : ils ne sont pas le seul public exposé aux dangers de la propagande étrangère]

La communauté des professionnels du jeu vidéo s'est saisie de la question de la protection des mineurs, notamment en les protégeant face aux contenus inappropriés. C'est avec l'exemple du système PEGI[57] qu'on peut arguer, preuve à l'appui, que la communauté est force de proposition et peut être soutenue par les acteurs institutionnels.

Pour protéger les mineurs, l'industrie du jeu vidéo a mis en place un système rating/classement des jeux vidéo. Le système dit « PEGI » (« Pan European Game Information », littéralement *« Information sur le jeu pan-européen »*) permet de trier les biens et services du jeu vidéo selon des catégories d'âges. Ce système permet ainsi aux parents, mais aussi au public mineur, de bénéficier de conseils, et d'être alertés, non pas sur la difficulté des jeux vidéo, mais sur leurs contenus (achat en

[56] *Code de bonnes pratiques 2022 en matière de désinformation*, téléchargeable en ligne sur :https://digital-strategy.ec.europa.eu/fr/policies/code-practice-disinformation

[57] **Pan european game information**, "Quelles sont les classifications "?, sur *pegi.info*, disponible en ligne sur : https://pegi.info/fr/page/quelles-sont-les-classifications

ligne, peur, violence, langage grossier, sexe, drogues, etc.), et ainsi d'orienter les consommateurs dans leurs achats et leur consommation.

La classification PEGI s'étend du PEGI 3 (pour les jeux qui conviennent aux enfants de 3 ans et plus) à PEGI 18 (pour les jeux qui conviennent aux enfants de 18 ans et plus). Le PEGI est utilisé dans l'ensemble de l'industrie européenne du jeu vidéo, et a bénéficié du soutien de la Commission européenne. La signalétique de cette harmonisation européenne est désormais obligatoire en France depuis 2015[58].

[1.4. Traiter le jeu vidéo comme un outil potentiel de propagande, et non plus seulement comme un objet de divertissement]

En considérant le jeu vidéo comme un objet politique, on envisage qu'il peut être particulièrement exposé à la propagande étrangère, qui se matérialise par le vol de données ou un détournement à des fins de désinformation :

- Concernant le vol des données dans l'industrie du jeu vidéo[59] : le Syndicat européen des développeurs de jeux vidéo (European Games Developper Federation, EGDF), dans sa communication générale, ainsi que lors d'une réponse à une consultation publique sur le Data Act, a publié un ensemble d'éléments reflétant les inquiétudes du secteur relatif aux données ainsi que de leurs utilisations par des services de renseignements étrangers. Ces appels sont relatifs au piratage et au vol des données, ainsi qu'aux immixtions étrangères dans les communautés des joueurs. Exemple de Angry Birds[60] : vol des données commerciales par les services secrets US et UK, notamment l'âge, la localisation et l'orientation sexuelle.
- Concernant la désinformation[61] : le Syndicat européen des développeurs de jeux vidéo alerte sur la nécessité de s'engager dans la lutte contre les faux comptes et les faux engagements, ainsi que les robots (les intelligences artificielles et autres 'bots') qui amplifient les engagements artificielles autours de récits faux, trompeurs ou haineux.

[1.5. Tenir compte de l'aspect protéiforme du jeu vidéo comme objet économique, culturel mais aussi politique]

[58] Loi n°2015-177 du 16 février 2015 - art. 22, entrée en vigueur le 18 février 2015, révisant l'article 32 de la loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

[59] **European Games Developper Federation**, "Safeguards against European and foreign intelligence services (2021)", disponible en ligne sur : https://www.egdf.eu/documentation/5-fair-digital-markets/how-to-regulate-data-economy-2020/the-union-has-to-defend-its-digital-industries-against-data-stealing-intelligence-services-2020/

[60] **BALL** James, "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data", in *The Guardian*, 28/01/2014, disponible en ligne sur : https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

[61] **European Games Developper Federation**, "Fighting online desinformation (2020)", disponible en ligne sur : https://www.egdf.eu/documentation/7-balanced-protection-of-vulnerable-players/fighting-online-disinformation/

Comme cela a été évoqué plus tôt, le jeu vidéo a été considéré par le politique comme un objet économique pour un marché de consommateur. Si on ne peut bien sûr pas contester cet état de fait, il convient pour autant de ne pas négliger l'aspect protéiforme du jeu vidéo, notamment son aspect culturel et politique.

Bien que le politique soit assez mal informé des questions relatives à l'industrie du jeu vidéo, l'inverse n'est pas vrai : l'industrie du jeu vidéo est très active sur le plan politique et international et a notamment œuvré économiquement et politiquement dans contexte conflictuel de la Guerre en Ukraine. Qu'on le veuille ou non, le jeu vidéo est politique et politisé. Ainsi, dans un communiqué du 26 février 2022, le vice-premier ministre Ukrainien Mykhailo Fedorov a interpellé l'ensemble des éditeurs et développeurs du jeu vidéo à annuler les événements ou à bloquer l'accès aux joueurs russes et biélorusses[62]. De nombreux professionnels ont répondu à l'appel en suspendant certaines ventes physiques et digitales, comme l'ont confirmé par exemple EA SPORT le 2 mars 2022 et Epic Games le 5 mars 2022. Au lendemain de ces sanctions, la Fédération de Russie a décidé de modifier sa réglementation nationale relative à la propriété intellectuelle, notamment en autorisant le "hacking" et le téléchargement illégal de jeux vidéo[63]. Cela est un énième risque d'une ingérence étrangère dans le milieu du jeu vidéo.

[1.6. Encourager une consultation européenne multi-parties prenantes dans laquelle le jeu vidéo serait analysé dans sa globalité (professionnels du secteur, joueurs, acteurs politiques, experts) afin de mener des actions concrètes susceptibles de permettre de protéger les jeux vidéo contre l'ingérence étrangère via le numérique]

Il est nécessaire que l'ensemble des acteurs publics et privés, directement ou indirectement concernés par la question du jeu vidéo, puissent participer à une consultation européenne multi-partie prenante. À l'issue de cette consultation, les parties prenantes doivent pouvoir être force de proposition afin de parvenir à un consensus politique, mais aussi à des actions qui permettront de développer des normes juridiques contraignantes pour les États-membres, pour les acteurs européens du numérique ainsi que les acteurs étrangers (privés ou publics). Une telle approche multidimensionnelle serait à même de permettre la protection des utilisateurs et joueurs contre les ingérences étrangères potentielles ou effectives via les outils numériques, et doit passer par (entres autres) :

---

[62] **ZAFFAGNI** Marc, "L'industrie du jeu vidéo réagit à la guerre en Ukraine : en Russie, les joueurs privés de grand Turismo 7", 07/03/2022, in futura-sciences.com, disponible sur : https://www.futura-sciences.com/tech/actualites/jeux-video-industrie-jeu-video-reagit-guerre-ukraine-russie-joueurs-prives-gran-turismo-7-97168/

[63] **MAXWELL** Andy, "Russia Will Probably Legalize Some Software Piracy to Mitigate Sanctions", in Torrentfreak.com, 07/03/2022, disponible en ligne sur : https://torrentfreak.com/russia-will-probably-legalize-some-software-piracy-to-mitigate-sanctions-220307/

- Consulter davantage les professionnels de l'industrie du numérique, y compris sur le secteur du jeu vidéo ;
- Consulter les juristes praticiens, ayant une expérience pratique de la mise en œuvre des législations ;
- Consulter les juristes universitaires ;
- Consulter la jeunesse.

2. *Empowerment* des communautés : il faut continuer de donner aux communautés de gameurs les moyens de se former pour favoriser une utilisation vertueuse du jeu vidéo

Pour que la communauté des joueurs puisse participer activement à la création d'un espace en ligne sain et sécurisé, il est nécessaire de leur transmettre les outils qui leur permettront de lutter contre les comportements haineux en leur sein, mais également de promouvoir un ensemble de valeurs vertueuses par le biais de leurs canaux

[2.1. Combattre les comportements toxiques et la haine en ligne]

Il est nécessaire de donner à la communauté des *gameurs* des moyens permettant de faire du jeu vidéo un espace où la haine en ligne n'a pas sa place. Cela passe notamment par un ensemble d'outils techniques.

En voici quelques exemples intéressants :

- Les **systèmes de signalement** permettent de "dénoncer" les comportements toxiques et haineux en ligne. Il s'agit d'un système reflétant le volontarisme de la communauté des joueurs : ce sont des particuliers qui dénoncent ces comportements à des modérateurs ou des administrateurs. La vigilance collective des joueurs est essentielle.

- Les **modérateurs** sont chargés de faire en sorte que les jeux et forums conservent une ambiance conviviale. Ils sont parfois bénévoles, parfois employés. Ils peuvent avertir d'éventuelles sanctions, et sanctionner le cas échéant lorsque la violation des règles est manifestement grave et/ou répétée.

- Au-delà de ces systèmes humains, les **logiciels de filtrage** permettent d'éliminer automatiquement certains comportements, expressions ou vocabulaire des fils de discussion (exemple : les insultes sont remplacées par des astérisques ; l'utilisation d'expression à caractère discriminatoire sont automatiquement reconnus par l'IA et un avertissement envoyé ou une sanction est directement prononcée).

- Lorsque l'ensemble des procédés ne permettent pas au joueur de bénéficier de l'expérience de jeu qu'il souhaite, il peut également mettre en **sourdine**

des joueurs ou le fil de discussion tout entier. Pour autant, il s'agit là de la dernière étape, car il est souvent déjà trop tard : le mal est déjà fait pour que le joueur doive en arriver là.

Malheureusement, ces outils ne sont pas toujours assez performants, et certaines attitudes toxiques échappent à ces signalisations, modérations et filtrages. Les attitudes haineuses, et les actes d'ingérences étrangères, se font toujours plus inventifs dans leur vocabulaire ou dans leur utilisation des failles des logiciels ou humains pour éviter ces procédés. Mais il s'agit au moins de commencer à faire la chasse à ce genre de pratique sur le terrain, et à promouvoir des valeurs positives.

[2.2. Promouvoir les valeurs de l'eSport][64]

Le jeu vidéo est un espace de partage de contenu, mais également de valeur. C'est en ce sens que la promotion des valeurs de l'eSport est essentielle afin que les joueurs deviennent responsables et qu'ils puissent co-construire une communauté accueillante, bienveillante, diversifiée et engageante. Ces valeurs doivent être partagées, respectées et encouragées par toutes les parties prenantes de l'environnement du jeu vidéo (joueurs amateurs, joueurs de compétition, professionnels de l'industrie, à l'échelle locale comme à l'échelle internationale).

Quatre piliers sont ainsi retenus par la Fédération européenne du jeu vidéo :

(i) la sécurité et le bien-être : s'efforcer à faire du jeu vidéo un espaces sûrs et exempts de menaces ou de violences, verbales ou physiques ;

(ii) l'intégrité et le fair-play : ne pas tricher, pirater ou se livrer à des comportements trompeurs ou malhonnête ;

(iii) le respect et la diversité : au-delà de la simple courtoisie, il s'agit d'encourager le jeu vidéo d'être un espace où se rencontrent différents milieux, différentes cultures et différentes perspectives. Il s'agit de faire du jeu vidéo un espace inclusif pour tous, quels que soient l'identité de genre, l'âge, les capacités, la race, les origines ethniques, la religion ou l'orientation sexuelle du joueur ;

(iv) le jeu positif et enrichissant : jouer doit être synonyme d'esprit d'équipe et de confiance en soi, mais aussi de développement de compétence comme la stratégie, la collaboration et l'esprit critique.

3. Pédagogie

[3.1. Sensibiliser dès le plus jeune âge à l'esprit critique et former le jeune public à détecter un contenu qui doit leur apparaître comme anormal]

[64] **Europe's game video industry**, "What are esports ?", disponible en ligne sur : https://www.isfe.eu/isfe-esports/

Sensibiliser le jeune public, tout au long de son apprentissage et de sa scolarité, à l'école et en dehors, à la formation de son esprit critique lui permet de détecter les informations et le contenu qui pourrait lui paraître comme anormal.

Si bien sûr on ne demandera jamais à un enfant de 10 ans de reconnaître du contenu issu de la propagande étrangère, il pourra néanmoins communiquer ses doutes à un adulte, qui sera ensuite en mesure de prendre les dispositions nécessaires et de faire les signalements appropriés.

C'est par exemple le chemin pris par la modification de la Loi Avia, qui modifie l'article du Code de l'Éducation relatif à la formation à l'utilisation des outils et des ressources numériques, en matière de lutte contre la diffusion des contenus haineux en ligne. L'idée serait de faire une modification similaire concernant la propagande étrangère.

[3.2. Sensibilisation des jeunes adultes dans les associations de joueurs, universités, entreprises]

Dans le prolongement de la proposition précédente, la sensibilisation doit être adressé aux enfants, mais pas que et doit donc se matérialiser :

- Dans les écoles
- Dans les universités
- Au sein des institutions, européennes et nationales
- Dans les associations
- Dans les entreprises