Clara asbl
Audiovisuel - Education Permanente

Etude

Pourrait-on davantage réglementer, par la loi, l'accès aux mineurs à certains contenus sur Internet ?

Jean-François Furnémont, Président du CLARA

1. Introduction

La violence, tout comme d'autres comportements, s'apprend par l'exposition visuelle. Il existe un lien de cause à effet entre le comportement agressif et le fait de voir de la violence. Comme le montrent les études, les élèves d'âge préscolaire et les adolescents qui consomment beaucoup de violence dans les médias sont plus agressifs que ceux qui sont des téléspectateurs légers[1]. L'exposition des enfants à la violence les désensibilise aux médias, tandis que la consommation de contenu médiatique violent inculque aux enfants l'idée qu'il s'agit de la nouvelle norme. La violence fait partie de la vie quotidienne et les rend moins sensibles émotionnellement à celle-ci.

De manière générale, le contenu que les enfants regardent a un impact sur leurs comportements futurs. Tous les enfants sont en ligne, via plus d'appareils et de services, plus fréquemment, pour plus d'activités, et à des âges de plus en plus jeunes. Internet et les développements technologiques qui l'accompagnent offrent d'énormes possibilités aux enfants en termes d'apprentissage et d'information, de divertissement et de jeu, de communication et de participation. De nombreuses activités en ligne ont un aspect positif et sont devenues aujourd'hui essentielles à la vie quotidienne, mais elles présentent également des risques pour la sécurité, le bien-être et aussi le respect des droits des mineurs.

La génération dite Alpha, née de 2010 à aujourd'hui, a été nommée ainsi car la nomenclature des lettres latines précédente a pris fin avec la génération dite Z ou Zoomers (née du milieu des années 1990 à 2009) et l'approche scientifique a été de poursuivre par la nomenclature grecque à la place, mais aussi de peut-être prophétiser symboliquement le désir non pas un retour à l'ancien, mais de marquer le début de quelque chose de nouveau[2].

La génération Alpha, tout comme la génération Z avant elle, est très habile à utiliser les outils numériques, mais elle manque de compréhension de leur usage, en particulier en ce qui concerne les normes sociales, les opportunités créatives et l'évaluation critique de la désinformation, de la persuasion, de l'exploitation ou de l'autoprotection. Les membres de cette génération sont, essentiellement, des cibles vulnérables pour ceux qui chercher à manipuler et à porter préjudice.

Tout comme nous comprenons l'importance (et tentons) de protéger les mineurs dans la vie réelle ou dans ce que l'on appelle maintenant le monde hors ligne, le même paradigme devrait s'appliquer dans le monde hors ligne. L'intimidation en ligne (cyberintimidation), l'atteinte à la vie privée, l'usurpation d'identité, l'exposition à des contenus offensants, les actes criminels générant soutien et acclamation, la honte en

[1] Huston, A.C., Donnerstein, E., Fairchild, H., Feshbach, N. D., Katz, P.A., Murray, J., Rubenstein, A. E., Wilcox, B.L., & Zuckerman, D. (1992). Big world, small screen. Lincoln: University of Nebraska Press, 1992, pp. 54-55.

[2] https://mccrindle.com.au/article/topic/generation-alpha/generation-alpha-defined/

ligne, le phishing[3], les publications en ligne qui hantent les enfants dans la vie réelle, la présence d'inconnus aux intentions malveillantes, mais aussi les « compétitions » d'automutilation, les abus sexuels sur les enfants, la radicalisation totale de certains jeunes, les meurtres et les suicides ne sont que quelques exemples d'expériences néfastes vécues par les enfants en ligne, mais elles se traduisent également dans la vie réelle.

Si nous ajoutons à cela le développement exponentiel de l'intelligence artificielle, avec des conséquences peut-être insondables sur nos mondes physiques, où même les adultes avertis ne parviennent pas à comprendre et à combattre les dommages qu'elle peut causer, il y a peu de place pour une vision optimiste des expériences en ligne qui soient sûres et positives.

De nombreuses tentatives d'établissement de mesures législatives de protection des mineurs en ligne sont mises en oeuvre, du moins dans la perspective de l'Union européenne, perspective qui sera développée dans cette étude. Couplée à un certain nombre de tendances et de réponses à ces mesures, cette étude fournira aussi des recommandations dans le but de faire de l'espace en ligne un espace amusant, créatif, d'apprentissage et d'épanouissement pour les enfants.

[3] Pratique frauduleuse consistant à envoyer des courriels ou d'autres messages prétendant provenir d'entreprises réputées afin d'inciter les individus à révéler des informations personnelles, telles que des mots de passe.

2. La protection des mineurs en ligne : une perspective européenne

D'un point de vue sociétal, l'année 2022 a été proclamée Année européenne de la jeunesse (AEJ22), afin de mettre en évidence et d'atténuer l'impact de la pandémie sur l'éducation, l'emploi, l'inclusion sociale et la santé mentale des jeunes, et d'offrir aux jeunes Européens la possibilité d'acquérir des connaissances et des compétences, ainsi que de renforcer leur engagement civique pour façonner l'avenir de l'Europe. L'Année visait également à renforcer la stratégie de l'Union européenne en faveur de la jeunesse pour la période 2019-2027[4].

Si l'on se concentre davantage sur le domaine des services de médias audiovisuels et de l'environnement en ligne, l'Union européenne semble être à l'avant-garde des efforts déployés pour relever les nombreux défis liés à la protection des mineurs en ligne, comme nous allons le développer ci-dessous.

2.1. La protection des mineurs dans le cadre de la directive révisée sur les services de médias audiovisuels

Les modifications apportées au cadre réglementaire européen par la Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels[5] (ci-après la Directive SMA révisée) ont mise en évidence la nécessité continue de trouver un équilibre entre la protection des publics vulnérables et la sauvegarde de la liberté d'expression, qui a toujours été l'un des principes fondamentaux de la législation en matière de médias.

C'est notamment le cas de la protection des mineurs, universellement reconnue comme l'une des priorités des politiques publiques médiatiques. Cette préoccupation était déjà présente dans l'environnement de la télévision linéaire, avec la mise en œuvre de mesures de protection telles que les systèmes de classification (signalétique) et les horaires de diffusion, qui ont été renforcées par la numérisation du paysage médiatique et l'émergence de platesformes qui ont permis une augmentation rapide du volume et du type de contenu disponible, ainsi que de nouveaux modèles de production, de distribution et d'accès aux de contenus.

[4] https://youth.europa.eu/strategy_fr
[5] https://eur-lex.europa.eu/eli/dir/2018/1808/oj?locale=fr

La Directive SMA révisée, reconnaissant la nécessité d'assurer une meilleure protection des mineurs contre les contenus préjudiciables dans le monde en ligne, peu importe les plateformes de distribution, a introduit deux changements majeurs dans les dispositions relatives à la protection des mineurs :

- l'harmonisation des normes de protection entre les services de médias audiovisuels linéaires (la télévision « classique ») et non linéaires (la vidéo à la demande, comme par exemple Netflix ou Disney+) ;
- l'extension de l'obligation de protection des mineurs aux plateformes de partage de vidéos, comme par exemple YouTube ou Dailymotion).

La notion de contenu préjudiciable est simplifiée et une approche antérieure à deux niveaux et graduée de la protection des mineurs a été remplacée par une nouvelle approche horizontale, applicable à tous les services de médias audiovisuels, en corrélation avec le niveau de préjudice.

Selon l'article 6 bis de la Directive SMA révisée, les mesures prises doivent être proportionnées au préjudice potentiel du programme et les États membres doivent veiller à ce que les fournisseurs de services *de médias « utilisent un système décrivant la nature potentiellement préjudiciable du contenu d'un service de médias audiovisuels ».* En outre, *« les contenus les plus préjudiciables, tels que la pornographie et la violence gratuite, feront l'objet des mesures les plus strictes »*.

Le considérant 20 de la Directive SMA révisée précise également que *« les contenus les plus préjudiciables qui, sans nécessairement constituer une infraction pénale, pourraient nuire à l'épanouissement physique, mental ou moral des mineurs, devraient faire l'objet des mesures les plus strictes, comme le cryptage et l'emploi d'outils de contrôle parental effectifs, sans préjudice de la possibilité pour les États membres d'adopter des mesures plus strictes »*.

TV + vidéo à la demande : **contenus *« qui pourraient nuire »* aux mineurs**	**TV + vidéo à la demande :** ***« contenus les plus préjudiciables »***
« ne sont mis à disposition que dans des conditions telles que les mineurs ne puissent normalement pas les entendre ni les voir » <u>Exemples de mesures</u> : Horaires de diffusion Signalétique Avertissement sonore Outils de vérification de l'âge	*« Les contenus les plus préjudiciables, tels que la violence gratuite et la pornographie, feront l'objet des mesures les plus strictes »* <u>Exemples de mesures</u> : Cryptage Outils de contrôle parental effectif

Plus particulièrement, la Directive SMAV révisée étend le champ d'application de la réglementation aux plateformes de partage de vidéos (PPV), qui sont définies de manière à inclure tous les principaux services en ligne, les réseaux sociaux, YouTube,

etc., qui devront également en termes de protection des mineurs prendre des mesures appropriées pour protéger les mineurs contre les programmes, les vidéos générées par les utilisateurs et les communications commerciales susceptibles de nuire à leur épanouissement physique, mental ou moral, mesures qui selon l'article 28 ter §3 *« sont déterminées en prenant en considération la nature du contenu en question, le préjudice qu'il pourrait causer, les caractéristiques de la catégorie des personnes à protéger ainsi que les droits et les intérêts légitimes en jeu »*.

Les mesures à mettre en œuvre par les PPV sont à la fois procédurales (par exemple, prévoir des mécanismes de plainte et de recours) et techniques (par exemple, la vérification de l'âge et les systèmes de contrôle parental). La mise en œuvre de ces mesures relève de la responsabilité des PPV, et une tâche d'évaluation spécifique est prévue pour les autorités nationales de régulation des médias, c'est-à-dire que l'autorité compétente évaluera l'opportunité des mesures prises par les PPV relevant de sa compétence territoriale.

Ces mesures doivent être proportionnées au niveau de préjudice (les contenus les plus préjudiciables doivent être soumis aux mesures de contrôle d'accès les plus strictes) et comprennent notamment :

- mettre en place et utiliser des mécanismes transparents et conviviaux permettant aux utilisateurs d'une plateforme d'indiquer ou de signaler au fournisseur de la plateforme concerné les contenus préjudiciables ;
- mettre en place et utiliser des systèmes permettant aux fournisseurs de plateformes d'expliquer aux utilisateurs de ces plateformes quelle suite a été donnée aux indications et aux signalisations ;
- mettre en place et utiliser des systèmes permettant de vérifier l'âge des utilisateurs des plateformes en ce qui concerne les contenus préjudiciables ;
- mettre en place et utiliser des systèmes faciles à utiliser permettant aux utilisateurs des plateformes de classifier les contenus préjudiciables ;
- prévoir des systèmes de contrôle parental dont les utilisateurs finaux ont le contrôle en ce qui concerne les contenus préjudiciables ;
- prévoir des mesures et des outils d'éducation aux médias efficaces et sensibiliser les utilisateurs à ces mesures et outils.

En outre, une référence spécifique à la protection des données des enfants est un ajout important : à l'article 6 bis, la Directive SMA révisée stipule que les données à caractère personnel des mineurs collectées ou générées d'une autre manière par les fournisseurs de services de médias *« ne sont pas traitées à des fins commerciales, telles que le démarchage, le profilage et la publicité basée sur le ciblage comportemental ».*

Pour rappel, dans son rapport *« Protection des mineurs dans les services de médias audiovisuels : tendances et pratiques »*[6], le Groupe des régulateurs européens des

[6] http://erga-online.eu/wp-content/uploads/2016/10/ERGA-PoM-Report-2017-wordpress.pdf

services de médias audiovisuels (ERGA)[7] a décrit les outils et mesures les plus utilisés dans les pays de l'Union européenne pour aider les parents à protéger les enfants contre les contenus susceptibles d'être inappropriés ou potentiellement préjudiciables à leur développement ou à leur bien-être général. Les schémas les plus couramment utilisés pour mettre en œuvre les mesures réglementaires de base sont les suivants :

- la fourniture d'informations sur le contenu, telles que les classifications par âge ou les descripteurs de contenu ;
- restreindre l'accès des mineurs par le biais de l'établissement d'un horaire de diffusion ;
- restreindre l'accès des mineurs par des mécanismes techniques.

Les informations sur le contenu sont utilisées pour indiquer la pertinence ou la nocivité du contenu pour le public. À cette fin, le système peut consister en des étiquettes de classification par âge (signalétique) qui indiquent l'aptitude ou la nocivité pour diverses catégories d'âge d'enfants. Il peut également être complété par des descripteurs de contenu indiquant les caractéristiques ou la nature pertinentes du contenu, qui peuvent prendre la forme d'étiquettes, d'indications textuelles et d'avertissements.

Les restrictions horaires sont utilisées pour réduire la probabilité que les mineurs soient exposés à des contenus potentiellement préjudiciables ou inappropriés. Il s'agit de restrictions sur le moment de la journée où le contenu peut être mis à disposition dans le cadre du service ou de restrictions sur le placement du contenu potentiellement préjudiciable à proximité d'autres contenus.

Les mesures techniques décrivent des mécanismes autres que la programmation utilisés pour réduire la probabilité que les mineurs soient exposés à des contenus potentiellement préjudiciables ou inappropriés, en plaçant une barrière technique entre l'utilisateur et le contenu. Les exemples les plus courants sont les différents types de contrôles parentaux, les codes PIN ou les outils de vérification de l'âge (contrôles de carte de crédit, preuves d'âge et contrôles de confirmation d'âge...).

En général, les fournisseurs de SMA sont en mesure d'inclure des informations sur le contenu en plus du contenu lui-même dans leurs services (par exemple avant le début d'un programme). Cependant, ils s'appuient souvent sur des tiers tels que des plateformes de télévision (distributeurs), des PPV et d'autres pour permettre l'application de mesures techniques au contenu de leurs services. De même, les fournisseurs de SMA s'appuient sur les opérateurs de guides électroniques de programmes (EPG) pour inclure des informations pertinentes sur le contenu, qu'il s'agisse d'étiquettes de classification par âge ou de directives textuelles.

En ce qui concerne les mesures les plus couramment utilisées en fonction du type de service, le rapport de l'ERGA souligne les éléments suivants :

- télévision (services linéaires) : les restrictions horaires et les informations sur le contenu sont les principaux outils utilisés pour la protection des mineurs dans

[7] L'ERGA rassemble des chefs ou des représentants de haut niveau d'organismes nationaux de régulation indépendants dans le domaine des services audiovisuels, afin de conseiller la Commission européenne sur la mise en œuvre de la Directive SMA.

l'environnement linéaire, car ils sont, au moins dans une certaine mesure, utilisés par la quasi-totalité des services linéaires de l'Union européenne. La pratique réelle varie toutefois d'un pays à l'autre. Seuls deux États membres n'ont pas d'obligation de signalétique (République tchèque et Danemark), alors que dans d'autres, cette obligation existe et relève soit de la législation (Belgique, Croatie, France, Hongrie, Slovaquie, Royaume-Uni, Norvège, …), soit d'un dispositif de corégulation (Pays-Bas, Finlande, Allemagne, Italie, Espagne, …).

- Vidéo à la demande (services non linéaires) : les restrictions horaires ne sont couramment pas utilisées, et quand elles le sont, c'est imposé par la législation. Les classifications d'âge sont plus couramment utilisées, ainsi que le contrôle parental. Habituellement, cela se fait à l'aide d'un code PIN que l'utilisateur doit saisir pour afficher un contenu réservé aux adultes. Un système de code PIN semble être une fonctionnalité standard, mais il existe également d'autres méthodes. L'exigence de la date de naissance lors de l'inscription est également considérée comme une méthode de contrôle parental pour empêcher les mineurs de s'inscrire immédiatement à un service. L'utilisation de catalogues spéciaux est un autre moyen : en France, par exemple, les fournisseurs de services de vidéo à la demande doivent fournir une *« zone de confiance »* qui permet aux familles et au jeune public de n'avoir accès qu'à des programmes sans classification d'âge. La quatrième mesure utilisée consiste à mettre en place des applications dédiées aux enfants qui permettent de ne regarder que du contenu pour enfants sur une plate-forme de vidéo à la demande particulière.
- Plateformes de partage de vidéos : vérification de l'âge (âge minimum requis pour posséder un compte), restriction d'âge (contenu non visible par les utilisateurs de moins de 18 ans), classification par âge (classification qui identifie le contenu réservé aux adultes), mode restreint (affichage uniquement de contenu adapté aux familles), applications pour enfants (par exemple, YouTube Kids).
- Distributeurs et plateformes : classification par âge fournie par le fournisseur du service (par exemple sur les guides électroniques de programmes), codes PIN (les plus utilisés), diverses mesures de contrôle parental.

La publication de l'Observatoire européen de l'audiovisuel sur la protection des mineurs dans un environnement médiatique convergent[8] énumère certaines mesures technologiques qui peuvent être introduites sur les services de télévision et de vidéo à la demande pour restreindre l'accès des enfants à certains contenus diffusés et à la demande :

- Il peut être procédé à une vérification initiale de l'âge via un examen en personne des papiers d'identité de l'acheteur (dans un commerce, par exemple), des contrôles approfondis d'informations le concernant dans une documentation ou une base de données, ou encore une simple autodéclaration.
- Les contrôles au jour le jour peuvent être effectués au moyen d'un code PIN, c'est-à-dire d'un code personnel secret (composé généralement de quatre

[8] https://rm.coe.int/1680783486

chiffres) exigé par le fournisseur pour empêcher les utilisateurs non autorisés d'accéder à certains contenus ; il est également possible d'instaurer une obligation de paiement par carte bancaire (« paywall ») avant de permettre l'accès au service.

- Les services de télévision peuvent être assortis de technologies de cryptage. Il s'agit de procédés technologiques grâce auxquels les contenus audiovisuels sont diffusés de telle façon que seuls certains utilisateurs (abonnés à un service de télévision à péage, par exemple) possédant la clé de déchiffrement (par exemple sous la forme d'un décodeur équipé d'une carte de décryptage) peuvent les visionner.
- Des systèmes techniques de filtrage peuvent être mis en oeuvre au niveau du logiciel ou du terminal, de façon à bloquer l'accès à certains contenus.

La mise en œuvre effective de ces dispositions n'en étant qu'à ses balbutiements, il est impossible, à l'heure actuelle d'évaluer de manière adéquate quels outils sont utilisés par les PPV. Toutefois, une indication des obligations législatives adoptées dans les États membres de l'Union européenne, à la suite de la transposition de la Directive SMA révisée, peut être trouvée dans la publication de l'Observatoire européen de l'audiovisuel qui cartographie les règles nationales applicables aux PPV relatives aux contenus illicites et préjudiciables en ligne[9]. Il en ressort que les obligations des PPV identifiées par la Directive SMAV révisée et détaillées ci-dessus se retrouvent dans la grande majorité des législations nationales. Outre l'interdiction de certains contenus (les plus préjudiciables) et l'interdiction de l'utilisation des données personnelles des mineurs à des fins commerciales, les législations nationales mettent l'accent sur la mise en œuvre de mesures techniques et de systèmes de signalement/notification, ainsi que sur l'obligation de veiller à ce que des systèmes efficaces soient mis en place pour traiter et résoudre les plaintes des utilisateurs. En ce qui concerne la faisabilité des mesures imposées aux PPV, un nombre important de pays appliquent les critères mentionnés dans la Directive SMAV révisée (énumérés ci-dessus). Cependant, certains pays ont adopté d'autres critères, tels que le préjudice causé par et l'illégalité du contenu, le champ d'application matériel des PPV ou stipulent que le fournisseur doit exercer un contrôle limité sur les communications et toute autre mesure qui a été prise ou doit être prise. Dans certains cas, il est indiqué que l'autorité de régulation nationale et/ou le gouvernement peuvent adopter des règles supplémentaires. D'ailleurs, une des conclusions de cette publication est que l'ampleur de la transposition de la Directive SMA révisée dépendra surtout de l'adoption ultérieure de législations secondaires par les Etats membres.

Un autre aspect récent des défis en ligne mérite d'être relevé. Le 25 octobre 2023, la Commission du marché intérieur et de la protection des consommateurs (IMCO) du Parlement européen a adopté un nouveau rapport important sur la conception addictive des services en ligne et la protection des consommateurs dans le marché unique de l'Union européenne[10]. Le rapport souligne notamment que la question de la conception addictive n'est pas suffisamment couverte par la législation européenne

[9] https://rm.coe.int/mapping-on-video-sharing-platforms-2021-full-report/1680a43575
[10] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2023/10-25/15-CAs_AddictiveDesignEN.pdf

existante et que, si elle n'est pas abordée, elle pourrait conduire à une nouvelle détérioration de la santé publique, en particulier chez les mineurs. Le rapport demande à la Commission européenne d'examiner les initiatives politiques nécessaires et de présenter une législation contre les produits créant une dépendance, lorsque cela est approprié et nécessaire.

Le rapport note que de nombreux services numériques, tels que les jeux en ligne, les médias sociaux, les services de streaming pour les films, les séries ou la musique, les marchés en ligne ou les boutiques en ligne et les applications de rencontres sont conçus pour que les utilisateurs restent le plus longtemps possible sur la plateforme afin de maximiser le temps et l'argent qu'ils y passent et que de nombreux services en ligne sont conçus pour créer une dépendance aussi forte que possible. En outre, le rapport s'alarme du fait que certaines plateformes et autres entreprises technologiques exploitent les vulnérabilités psychologiques pour concevoir des interfaces numériques à des fins commerciales qui maximisent la fréquence et la durée des visites des utilisateurs, de manière à prolonger l'utilisation des services en ligne et à créer un engagement avec la plateforme.

Le rapport invite la Commission européenne à examiner quelles initiatives politiques sont nécessaires et à présenter une législation contre la conception addictive, le cas échéant et si nécessaire. Notamment, si le sujet reste sans réponse, le Parlement devrait être « le premier à agir et à faire usage de son droit d'initiative législative ». En outre, le rapport exige que la Commission, dans le cadre de son examen de la législation européenne existante en matière de design addictif, propose un « droit à ne pas être dérangé » numérique afin de donner aux consommateurs le pouvoir de désactiver, dès la conception, toutes les fonctions qui attirent l'attention. Le rapport invite également la Commission à promouvoir une conception éthique des services en ligne par défaut et à dresser une liste de bonnes pratiques en matière d'éléments de conception qui ne créent pas de dépendance ou de manipulation et qui garantissent que les utilisateurs gardent le contrôle et puissent prendre des mesures conscientes et informées en ligne sans être confrontés à une surcharge d'informations ou à une influence subconsciente. Enfin, la Commission réexamine actuellement la Directive sur les pratiques commerciales déloyales, la Directive sur les droits des consommateurs et la Directive sur les clauses contractuelles abusives. Le rapport invite instamment la Commission à garantir un niveau élevé de protection dans l'environnement numérique en veillant à s'attaquer aux problèmes croissants liés à la conception des services en ligne qui créent une dépendance, qui influencent le comportement et qui sont manipulateurs.

2.2. Exemples d'approches législatives plus larges en matière de sécurité en ligne

2.2.1. Irlande

L'Irlande est l'État membre de l'Union européenne qui a la compétence territoriale sur les principales PPV (YouTube, Facebook, Instagram, TikTok, …). La législation irlandaise sur la sécurité en ligne et la réglementation des médias (OSMR)[11], adoptée fin 2022, témoigne des efforts considérables déployés par l'Etat irlandais pour désormais enfin lutter contre les contenus préjudiciables en ligne.

Elle vise à répondre à de multiples préoccupations en ligne et traite de trois domaines principaux. Elle établit une nouvelle Commission des médias[12], dotée de pouvoirs fortement accrus allant jusqu'à pouvoir sanctionner les plateformes numériques et, si nécessaire, bloquer l'accès à certaines d'entre elles. Ce nouveau cadre législatif comprend la création d'un poste dédé de Commissaire à la sécurité en ligne au sein de la Commission des médias, chargé d'élaborer des codes de sécurité en ligne régissant les normes et les pratiques qui doivent être respectées par les services en ligne désignés par la Commission Les codes de sécurité en ligne devront prévoir les mesures à prendre par les services en ligne désignés pour réduire au minimum la disponibilité de contenus en ligne préjudiciables, les mesures à prendre en ce qui concerne les communications commerciales disponibles sur leurs services, les mécanismes de traitement des plaintes des utilisateurs, les évaluations des risques et de l'impact à effectuer par les services en ligne désignés en ce qui concerne la disponibilité de contenus préjudiciables.

Certains observateurs de ces développements législatifs pointent le risque que cette législation puisse aboutir des mesures de restriction de la liberté d'expression. Une autre préoccupation concerne la manière dont la Commission des médias identifiera et définira de nouvelles catégories de contenus préjudiciables. Quoi qu'il en soit, étant donné que cette législation vient d'entrer en vigueur et que la nouvelle Commission des médias est en train de se mettre en place, il reste à voir comment et dans quelle mesure cette approche contribuera à réduire les préjudices en ligne, et en particulier à renforcer la protection des mineurs dans le monde en ligne.

2.2.2. France

En France, l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)[13] a été créée le 1er janvier 2022 par la fusion du CSA (ancien régulateur des médias) et de l'HADOPI (ancien régulateur des droits d'auteur en ligne). Les obligations et compétences de l'Arcom vis-à-vis des PPV consistent notamment à s'assurer que celles-ci prennent les mesures appropriées pour que les programmes, les vidéos créées par les utilisateurs et les communications commerciales audiovisuelles qu'ils fournissent soient conformes aux dispositions pertinentes (relatives à la protection des mineurs et du public en général contre certains contenus préjudiciables) et aux règles imposées aux communications commerciales audiovisuelles qu'elles commercialisent, vendent ou organisent elles-mêmes.

[11] https://www.oireachtas.ie/en/bills/bill/2022/6/
[12] https://www.cnam.ie/online-safety/
[13] https://www.arcom.fr/

L'Arcom établit et tient à jour une liste des PPV relevant de la compétence territoriale française, en indiquant le critère sur lequel cette compétence est fondée. En cas de litige entre l'utilisateur et les PPV, l'Arcom peut statuer sur les litiges entre l'utilisateur et les VSP relatifs à l'application des obligations découlant de la transposition de la Directive SMAV révisée. Il statue dans un délai de 2 à 4 mois et peut mettre en œuvre les mesures prévues en cas de non-respect des obligations.

L'Arcom encourage également l'adoption des codes et chartes suivants par les PPV :

- codes de bonne conduite destinés à l'adoption des mesures obligatoires ;
- chartes visant à encadrer l'exploitation commerciale de l'image des enfants de moins de 16 ans sur les plateformes en ligne ;
- codes de bonne conduite visant à réduire efficacement l'exposition des enfants aux communications commerciales audiovisuelles relatives à des denrées alimentaires ou des boissons contenant des nutriments ou des substances ayant un effet nutritionnel ou physiologique, notamment les matières grasses, les acides gras trans, le sel ou sodium et les sucres, dont la présence en quantités excessives dans le régime alimentaire global n'est pas recommandée ;
- « contrats climats » ayant notamment pour objet de réduire de manière significative les communications commerciales sur les services audiovisuels et les PPV relatives à des biens et services ayant un impact négatif sur l'environnement.

Enfin, il est intéressant de noter que le 17 octobre 2023, l'Assemblée nationale française a adopté en première lecture le projet de loi visant à sécuriser et réguler l'espace numérique, qui avait déjà été adopté en première lecture par le Sénat le 7 juillet. Dans le cadre de la procédure accélérée engagée par le gouvernement, une commission mixte paritaire devrait maintenant se réunir, probablement en décembre 2023.

Ce texte législatif très ambitieux vise à renforcer la protection des mineurs en ligne et des citoyens dans le monde numérique. Il confère à l'Arcom de nouvelles compétences pour contrôler l'accessibilité de la pornographie en ligne aux mineurs et pour définir les exigences techniques auxquelles doivent répondre les systèmes de vérification de l'âge qui restreignent l'accès à ces contenus. Au cours de leurs délibérations, les membres de l'Assemblée nationale ont étendu les exigences en matière de vérification de l'âge aux services de jeux d'argent en ligne. Le texte adopté inclut la procédure de mise en demeure et de sanction pour les entreprises qui ne respectent pas les exigences de l'Arcom, et fixe les amendes maximales en cas de récidive pour les fournisseurs d'accès à Internet, les moteurs de recherche ou les annuaires (150.000 euros ou 2% du chiffre d'affaires mondial) et les éditeurs (500.000 euros ou 6% du chiffre d'affaires mondial). Après l'article 3, qui sanctionne les hébergeurs qui ne se conforment pas à une demande de retrait de pornographie enfantine, un article supplémentaire a été créé, qui étend l'obligation de retrait des hébergeurs aux contenus à caractère sexuel impliquant des adultes et diffusés sans leur consentement. Si la pédopornographie doit être retirée dans les 24 heures suivant

la réception d'une injonction de l'autorité administrative, les contenus impliquant des adultes doivent être retirés dans un délai de sept jours[14].

2.2.3. Royaume-Uni

La loi britannique sur la sécurité en ligne[15], finalement adoptée le 19 septembre 2023, après trois ans de rédaction et de discussion, constitue un nouveau cadre réglementaire qui définit les mesures prises par le gouvernement pour lutter contre les contenus ou les activités en ligne qui nuisent aux utilisateurs individuels, en particulier aux enfants, et qui sont censés être, selon le gouvernement anglais, la législation de protection de l'enfance *« la plus puissante depuis une génération, tout en veillant à ce que les adultes soient mieux habilités à prendre le contrôle de leur vie en ligne et en protégeant notre santé mentale »*.

La loi rend les plateformes de médias sociaux responsables du contenu qu'elles hébergent et responsables, entre autres, de la sécurité des enfants et des jeunes en ligne, en étant obligées de supprimer rapidement les contenus illégaux ou de les empêcher d'apparaître en premier lieu, y compris les contenus faisant la promotion de l'automutilation. Elle requiert aussi d'empêcher les enfants d'accéder à des contenus préjudiciables et inappropriés pour leur âge, de faire respecter les limites d'âge et les mesures de vérification de l'âge, et de veiller à ce que les risques et les dangers posés aux enfants sur les plus grandes plateformes de médias sociaux soient plus transparents, notamment en publiant des évaluations des risques, tout en offrant aux parents et aux enfants des moyens clairs et accessibles de signaler les problèmes en ligne lorsqu'ils surviennent.

Si les plateformes de médias sociaux ne se conforment pas à ces règles, l'autorité de régulation (Ofccom) peut leur infliger une amende pouvant aller jusqu'à 18 millions de livres sterling ou 10 % de leur chiffre d'affaires annuel mondial, selon le montant le plus élevé, ce qui signifie que les amendes infligées aux plus grandes plateformes pourraient atteindre des milliards de livres.

En ce qui concerne plus particulièrement l'accès des enfants à des contenus inappropriés, certains des domaines que l'Ofcom s'attend à inclure dans un code de bonnes pratiques sont les suivants :

- les mesures que les entreprises doivent prendre pour s'assurer que leurs services sont sûrs dès la conception ; il peut s'agir par exemple de la mise à disposition de comptes avec des paramètres différents pour les enfants ;
- les conditions d'utilisation doivent indiquer clairement quels comportements et activités sont tolérés sur le service et les mesures mises en place pour empêcher les enfants d'accéder à des contenus inappropriés, et elles doivent être faciles à comprendre pour les enfants et les parents ;

[14] https://www.assemblee-nationale.fr/dyn/16/textes/l16t0175_texte-adopte-seance
[15] https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law

- les mesures que les entreprises doivent prendre pour s'assurer que les enfants ne peuvent pas accéder à des contenus inappropriés, y compris des conseils sur la vérification de l'âge, des avertissements de contenu et des mesures pour filtrer et bloquer les contenus inappropriés ;
- les mesures visant à s'assurer que les processus de signalement sont adaptés à l'objectif visé par la lutte contre ce préjudice et qu'ils sont clairs, visibles et faciles à comprendre pour les enfants et les parents ; les utilisateurs doivent aussi recevoir des explications claires sur les décisions prises par les plateformes ;
- les services disposent de processus efficaces et transparents pour modérer les contenus ; les utilisateurs sont tenus au courant de l'avancement de leur signalement ;
- les plateformes doivent prendre des mesures pour s'assurer que les préjudices sont rapidement traités, comme la suppression du contenu qui enfreint les conditions d'utilisation ;
- les processus que les plateformes doivent mettre en place pour s'assurer que les utilisateurs peuvent faire appel de la décision de suppression de leur contenu, afin de protéger les droits des utilisateurs en ligne ;
- les mesures visant à empêcher les utilisateurs bannis de créer de nouveaux comptes afin de continuer à créer du contenu inapproprié qui enfreint les conditions d'utilisation.

Il existe déjà quelques indicateurs préliminaires quant au niveau de respect de ces mesures, même si elles viennent seulement d'être rendues obligatoires. En effet, le rapport de l'Ofcom sur les principales conclusions de la première année de réglementation des PPV, d'octobre 2021 à octobre 2022, sur la base de la transposition de la Directive SMA révisée avant le Brexit[16], introduite dans la loi britannique sur les communications, en tenant compte des informations provenant des PPV, y compris, par exemple TikTok, Snapchat, Twitch, Vimeo, etc. a permis de constater que toutes les plateformes ont mis en place des mesures de sécurité, y compris des règles sur les types qui sont autorisées à être mises en ligne. Certaines plateformes ont apporté des modifications à leurs mesures en réponse directe au fait d'être réglementées dans le cadre du nouveau régime relatif aux PPV. Par contre, les plateformes ont généralement fourni des preuves limitées de l'efficacité de leurs mesures de sécurité pour protéger les utilisateurs. Il est donc difficile de déterminer avec certitude si les mesures de sécurité des PPV fonctionnent de manière cohérente et efficace. L'Ofcom estime que des mesures plus robustes sont nécessaires pour empêcher les enfants d'accéder à la pornographie, car il a été évalué que les mesures de contrôle d'accès de certaines PPV pour adultes ne sont pas suffisamment robustes pour empêcher les enfants d'accéder à la pornographie. De plus, le manque de connaissances, d'expertise et la volonté d'investir pour mieux se préparer à la réglementation ont été notés chez les PPV, y compris la réactivité limitée aux demandes formulées par les autorités de régulation. Enfin, et c'est peut-être le plus important, l'Ofcom a noté que les plates-formes *« ne donnent pas la priorité aux processus d'évaluation des risques, ce qui, selon l'Ofcom, est fondamental pour*

[16] https://www.ofcom.org.uk/__data/assets/pdf_file/0032/245579/2022-vsp-report.pdf

identifier et atténuer de manière proactive les risques pour la sécurité des utilisateurs »[17].

Après cette première année d'examen, l'Ofcom a commencé à mettre en œuvre activement les règles applicables. En ce sens, il convient de mentionner que le 10 novembre 2023, l'Ofcom a ouvert une enquête sur la société My Media World Ltd, en ce qui concerne la PPV Onevsp (anciennement connu sous le nom de Brand New Tube), en tenant compte de son respect de ses obligations légales en tant que fournisseur d'une PPV. En particulier, l'évaluation s'est concentrée sur les mesures selon lesquelles une PPV doit prendre et mettre en œuvre les mesures appropriées pour protéger les personnes de moins de 18 ans contre les vidéos contenant du contenus interdits au grand public (« restricted material ») ce qui inclut le contenu pornographique et d'autres contenus préjudiciables comme les contenus susceptibles d'inciter à la violence ou à la haine ou les contenus qui constitueraient une infraction pénale en vertu des lois relatives au terrorisme, à l'exploitation et à l'abus sexuels des enfants, ainsi qu'au racisme et à la xénophobie. Les règles applicables, comme indiqué précédemment, prévoient entre autres l'inclusion de conditions générales d'utilisation selon lesquelles si une personne met en ligne une vidéo sur le service qui contient de tels contenus, elle doit la porter à l'attention du fournisseur du service. L'Ofcom s'inquiète de la mise en œuvre et de l'efficacité des conditions d'utilisation de Onevsp. L'enquête examinera donc s'il existe des motifs raisonnables de croire que la société My Media World n'a pas pris et/ou mis en œuvre les mesures pour protéger ses utilisateurs contre les contenus préjudiciables pertinents et/ou les moins de 18 ans contre du contenu interdit au grand public[18].

[17] Ibid.

[18] https://www.ofcom.org.uk/about-ofcom/bulletins/enforcement-bulletin/open-cases/investigation-into-my-media-world-ltd?utm_medium=email&utm_campaign=My%20Media%20World%20investigation&utm_content=My%20Media%20World%20investigation+CID_f688db946158a0ba851e7d5e00cf5838&utm_source=updates&utm_term=opened%20an%20investigation.

3. Le paquet législatif de l'Union européenne sur les services numériques

L'adoption en 2022 de la législation sur les services numériques (Digital Services Act – DSA) et de la législation sur les marchés numériques (Digital Markets Act - DMA)[19], qui visent à créer un espace numérique plus sûr où les droits fondamentaux des utilisateurs sont protégés et à créer des conditions de concurrence équitables pour les entreprises, a été saluée comme une étape historique vers la réglementation de l'espace numérique.

Le DSA et le DMA représentent en effet une étape importante dans l'approche de la réglementation d'internet. Ses objectifs sont de créer un environnement en ligne plus sûr, d'identifier clairement la responsabilité des plateformes identifiées comme des places de marché en ligne et de relever les défis actuels de l'environnement numérique, notamment en ce qui concerne les produits et activités illégaux, les discours de haine et la désinformation, ainsi que la protection des données personnelles.

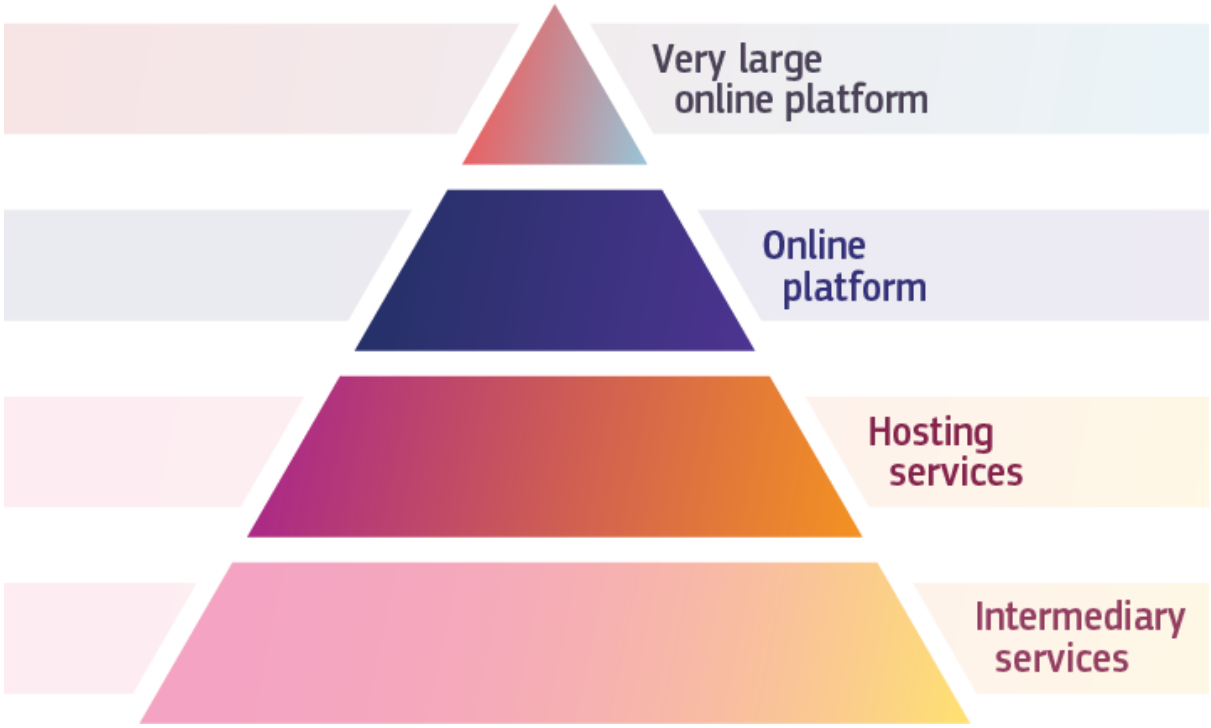
Les plateformes telles que Facebook, Google et Amazon seront désormais contraintes de mieux traiter les contenus illégaux et préjudiciables, de mieux protéger les utilisateurs et leurs droits fondamentaux, mais aussi de rendre transparentes leurs pratiques de modération des contenus et les algorithmes utilisés pour recommander des contenus.

Le DSA s'applique à tous les intermédiaires en ligne :

- Les très grandes plateformes en ligne et les moteurs de recherche qui présentent des risques particuliers pour la diffusion de contenus illicites et de préjudices pour la société. Des règles spécifiques sont prévues pour les plateformes atteignant plus de 10 % des 450 millions de consommateurs en Europe. La liste des plateformes désignées est disponible sur DSA: Très grandes plateformes en ligne et moteurs de recherche. Les très grandes plateformes en ligne et les moteurs de recherche présentent des risques particuliers pour la diffusion de contenus illicites et de préjudices pour la société. Des règles spécifiques sont prévues pour les plateformes atteignant plus de 10 % des 450 millions de consommateurs en Europe. La liste des plateformes désignées en avril 2023 par la Commission européenne compte 17 grandes plateformes en ligne (dont notamment Amazon store, Apple App Store, Facebook, Google Play, Instagram, Snapchat, TitTok, Twitter et Youtube) et deux moteurs de recherche (Microsoft Bing et Google Search)[20].

[19] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fr?etrans=fr
[20] https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_2413

- Les plateformes en ligne qui rassemblent les vendeurs et les consommateurs tels que les places de marché en ligne, les magasins d'applications, les plateformes d'économie collaborative et les plateformes de médias sociaux.
- Les services d'hébergement tels que le cloud et les services d'hébergement web (y compris les plateformes en ligne).
- Les services intermédiaires offrant une infrastructure de réseau: fournisseurs d'accès à Internet et bureaux d'enregistrement des noms de domaine (y compris les services d'hébergement).



Toutes les entreprises fournissant de tels services dans l'Union européenne sont désormais soumises à des obligations en vertu de la législation sur les services numériques, qu'elles soient établies sur son territoire ou non. Par conséquent, elle s'applique également aux plateformes établies en dehors de l'Union européenne, car chaque plateforme fournissant des services dans l'Union européenne devra y désigner un représentant légal, et la compétence territoriale sera déterminée en fonction du lieu où se trouve ce représentant.

Les obligations des différents acteurs en ligne seront proportionnelles à leur nature, à leur taille et au nombre d'utilisateurs, et généralement à leur rôle et à leur impact. Ainsi, les plateformes en ligne auront plus d'obligations que les catégories techniques d'intermédiaires en ligne, tandis que les exigences les plus strictes s'appliqueront aux très grandes plateformes en ligne et aux moteurs de recherche.

3.1. Les intermédiaires en ligne

Le DSA est un instrument juridique complexe, ambitieux et, du point de vue du mécanisme de surveillance, novateur. Il ambitionne d'aller au cœur même des problèmes du monde en ligne et introduit la responsabilité des intermédiaires en ligne, en particulier des plateformes en ligne telles que les réseaux sociaux et les places de marché en ligne, qui contrôlent l'accès au contenu, aux biens et aux services pour les publics, les consommateurs et les autres acteurs du marché. En effet, ces entreprises, dont le modèle économique est basé sur la maximisation de l'engagement des utilisateurs grâce à des algorithmes et des systèmes de recherche et de référence, dictent de fait la disponibilité et la visibilité du contenu.

En ce qui concerne la responsabilité en cas de diffusion de contenus illicites, le régime de responsabilité limitée établi en 2000 par la Directive sur le commerce électronique continue de s'appliquer aux plateformes en ligne : elles ne sont pas responsables du contenu illégal publié par les utilisateurs si elles n'ont pas connaissance d'activités ou d'informations illégales et agissent immédiatement dès qu'elles en ont connaissance et suppriment ces activités ou informations ou en empêchent l'accès. Par contre, l'ancienne limitation de responsabilité de la plateforme en ligne, dans le sens où son rôle était purement technique, automatique et passif, c'est-à-dire qu'elle n'a aucune connaissance ou aucun contrôle sur les données qu'elle stocke, ne s'applique plus. Leur rôle est désormais actif, et la limitation de responsabilité ne s'applique pas lorsque la plateforme s'occupe d'activités telles que le filtrage, la sélection, l'organisation, la promotion de certains contenus, etc.

C'est pourquoi les plateformes numériques ne peuvent plus être considérées comme des intermédiaires neutres et passifs, car elles influencent et déterminent la manière dont les contenus sont distribués et finalement consommés par les utilisateurs, et réalisent grâce à cela d'énormes bénéfices.

3.2. Qu'est-ce que le DSA ?

Contrairement aux précédentes tentatives de réglementation des services internet qui traitaient des conséquences plutôt que des causes, la législation sur les services numériques adopte une approche systématique pour lutter contre les abus en ligne et protéger les valeurs humaines fondamentales à l'ère numérique, en ciblant le problème central – le fonctionnement de ces entreprises, ou plus précisément leur modèle économique.

Il établit également un système de contrôle et d'application de la loi, qui prévoit la possibilité d'imposer des sanctions d'un montant de 6 % du chiffre d'affaires annuel mondial, tandis que des violations graves et répétées sont susceptibles d'aboutir à une interdiction d'opérer sur le territoire de l'Union européenne.

La Commission européenne s'est vu attribuer un rôle de contrôle extraordinaire en termes de compétence exclusive pour la surveillance des très grandes plateformes et des moteurs de recherche. Ils feront l'objet d'un suivi au niveau européen, en coopération avec les États membres. Les autres acteurs couverts par la législation relèvent de la compétence des États membres dans lesquels ces acteurs sont établis. Chaque Etat membre doit désigner un coordinateur des services numériques, un organe qui disposera de pouvoirs d'enquête et d'exécution pour mettre en œuvre les obligations et les exigences de la législation européenne au niveau national, et avec lequel les plateformes devront coopérer. Par exemple, la nouvelle Commission irlandaise des médias, la CNAM, nouvellement créée et évoquée ci-dessus, a été désignée comme coordinateur des services numériques et jouera un rôle clé de supervision dans l'application de cette loi en Irlande, pays qui héberge un grand nombre de plateformes numériques. En Belgique, il s'agira de l'Institut belge des services postaux et des télécommunications – IBPT[21]. Le soutien aux coordinateurs nationaux sera assuré par un nouvel organe à l'échelle de l'Union européenne, le Conseil européen des services numériques, dont le rôle sera consultatif.

Ce qui est important pour la préservation de la liberté d'expression, c'est que le DSA maintient le principe de la responsabilité limitée des hébergeurs pour les contenus dont ils n'ont pas connaissance, ainsi que l'absence d'obligation de surveiller activement la légalité des contenus qu'ils stockent.

Les nouvelles obligations des intermédiaires de l'internet sont les suivantes :

3.2.1. Mesures de lutte contre les biens, services et contenus illicites en ligne

Les plateformes en ligne seront obligées de mettre en place des mécanismes simples et facilement accessibles pour signaler les contenus considérés comme illégaux par les utilisateurs. Les utilisateurs devront recevoir une réponse au sujet de toutes les étapes de leur demande, y compris une notification de la décision finale et une explication détaillée de cette décision. Le traitement des demandes soumises par les tiers de confiance (« trusted flaggers ») sera prioritaire. Le statut de tiers de confiance est accordé par le coordinateur national des services numériques aux entités qui ont démontré qu'elles possèdent une expertise spécifique et la capacité nécessaire pour lutter contre les contenus illicites, représenter les intérêts collectifs et travailler de manière consciencieuse et objective.

Les décisions relatives à la suppression ou au blocage de certains contenus et leurs justifications seront rendues publiques dans une base de données gérée par la Commission européenne. En outre, les plateformes seront tenues de signaler les infractions présumées aux autorités compétentes, tandis que les autorités compétentes – tribunaux et coordinateurs nationaux – auront la compétence de demander la suppression de contenus illégaux conformément aux lois nationales ou

[21] https://ibpt.be/consommateurs

européennes, ainsi que de demander des informations sur les comptes des utilisateurs concernés.

Des obligations spécifiques pour les places de marché en ligne telles qu'Amazon, Airbnb, eBay, AliExpress et Etsy sont également envisagées afin d'empêcher la vente de biens et de services illégaux et contrefaits, compte tenu du rôle important que jouent ces plateformes dans la vie quotidienne des consommateurs européens. Des obligations s'appliquent à la collecte d'informations et à la vérification aléatoire de la crédibilité des tiers utilisant leurs plateformes.

3.2.2. Mesures de protection des utilisateurs, y compris la possibilité de s'opposer aux décisions des plateformes en matière de modération des contenus

La législation sur les services numériques définit les conditions dans lesquelles les plateformes en ligne pourront suspendre la fourniture de services, c'est-à-dire suspendre les comptes utilisateurs. Cela ne sera possible que pour les utilisateurs qui fournissent fréquemment des contenus clairement illégaux. La suspension ne peut être que temporaire et avec un avertissement préalable.

Les utilisateurs auront la possibilité de contester les décisions relatives à la suppression ou à l'incapacité de l'accès à l'information, les décisions de suspendre ou de mettre fin à la fourniture du service, et les décisions de suspension ou de résiliation du compte de l'utilisateur.

Dans un premier temps, les plateformes devront mettre en place des systèmes internes de traitement des plaintes, c'est-à-dire permettre aux utilisateurs de déposer une plainte facilement, électroniquement et librement dans un délai d'au moins 6 mois à compter de la décision de supprimer des contenus, de désactiver l'accès ou de bloquer le compte utilisateur. Les plateformes sont tenues d'informer les plaignants de la décision qu'ils ont prise en cas d'appel, ainsi que de la possibilité d'un règlement extrajudiciaire des litiges et d'autres options de protection juridique disponibles.

Dans le second cas, le règlement extrajudiciaire des litiges pourrait être effectué par un organe indépendant et expert dans le cadre de procédures administratives. Ces organismes seront agréés par le coordinateur national des services numériques, et leurs décisions seront contraignantes pour les plateformes.

3.2.3. Transparence des pratiques de modération et des systèmes de recommandation

Les plateformes en ligne seront tenues de soumettre des rapports sur les activités de modération des contenus, y compris des informations sur les ordres de suppression de contenus reçus des autorités nationales compétentes ou les notifications reçues des utilisateurs, un aperçu détaillé de la modération de contenu auto-initiée (nombre et expertise du personnel, langues avec lesquelles ils travaillent, nombre et type de

mesures prises) et du traitement des plaintes. Elles devront également rendre compte de l'utilisation de l'intelligence artificielle à des fins de modération automatique des contenus, ainsi que des informations sur l'objectif, les indicateurs de précision et les mesures de protection appliquées.

À la demande du coordinateur des services numériques, les plateformes devront permettre aux chercheurs ou aux universitaires d'accéder à des données dans le but de mener des recherches qui contribuent à l'identification et à la compréhension des risques systémiques, y compris les données sur le fonctionnement des algorithmes utilisés pour recommander du contenu ou des produits aux utilisateurs. Les informations confidentielles peuvent être omises des rapports accessibles au public, mais doivent être mises à la disposition des coordinateurs nationaux des services numériques et de la Commission européenne. Il n'y aura aucune possibilité d'exception fondée sur les secrets commerciaux.

3.2.4. Règles relatives à la publicité ciblée

Les utilisateurs auront un meilleur contrôle sur l'utilisation de leurs données personnelles et sur la manière dont elles sont monétisées ou utilisées pour de la publicité ciblée. Les très grandes plateformes et les moteurs de recherche devront offrir aux utilisateurs un système de recommandation de contenu qui ne soit pas basé sur leur profilage. Ils seront également tenus de divulguer les paramètres selon lesquels les utilisateurs se voient recommander certains contenus et services. Cela signifie, par exemple, que les utilisateurs doivent comprendre pourquoi leur contenu sur le fil d'actualité est trié d'une certaine manière, mais aussi qu'ils doivent avoir la possibilité de choisir comment le contenu leur sera présenté, par exemple en choisissant de l’afficher d’une manière chronologique plutôt qu'algorithmique.

Les plateformes ne seront pas autorisées à afficher des publicités ciblées basées sur les informations personnelles des mineurs, et le profilage des utilisateurs sur la base de données sensibles telles que l'origine ethnique, l'orientation sexuelle, les convictions religieuses ou politiques sera interdit.

Enfin, il sera interdit d'utiliser ce que l'on appelle des dark patterns, des pratiques déroutantes ou trompeuses (par exemple, sous forme de pop-ups) qui amènent les utilisateurs à choisir un service, un produit ou un contenu particulier.

3.2.5. Contenus préjudiciables : évaluation et atténuation des risques systémiques et codes de conduite

Bien que les obligations en matière de modération des contenus et de suppression/blocage des contenus concernent les contenus illégaux, le DSA touche également à la catégorie des contenus préjudiciables de plusieurs manières. Tout d'abord, si le contenu en question est soumis à des conditions d'utilisation ou à des normes communautaires, il relève alors des obligations de transparence concernant les pratiques de modération. Les très grandes plateformes en ligne et les moteurs de

recherche auront, en outre, l'obligation d'identifier et d'évaluer annuellement tous les risques systémiques importants découlant du fonctionnement et de l'utilisation de leurs services (c'est-à-dire la conception de la plateforme, le modèle d'affaires, les conditions commerciales, les normes communautaires, les systèmes de modération et de recommandation de contenu, le profilage des utilisateurs, les algorithmes...), concernant :

- La diffusion de contenus illégaux ;
- Les effets négatifs réels et anticipés sur les droits fondamentaux, y compris la protection des consommateurs, le respect de la dignité humaine, de la vie privée et familiale, la protection des données personnelles et la liberté d'expression et d'information, la liberté et le pluralisme des médias, l'interdiction de la discrimination, le droit à l'égalité des sexes et les droits de l'enfant ;
- des erreurs dans le fonctionnement ou des manipulations délibérées de leurs services, y compris des comptes utilisateurs frauduleux ou une exploitation automatisée du service (bots), pouvant conduire à la diffusion de contenus illicites ou de tout autre contenu ayant des effets négatifs réels et anticipés sur la protection des mineurs, les valeurs démocratiques, la liberté des médias, la liberté d'expression et le discours citoyen, les processus électoraux et la sécurité publique ;
- les conséquences négatives réelles et prévisibles pour la protection de la santé publique ainsi que d'autres conséquences négatives graves pour le bien-être physique, mental, social et financier des usagers.

Après avoir identifié les risques, les plateformes devront appliquer des mesures pour les atténuer, par exemple pour adapter leurs systèmes de modération ou de recommandation de contenus, le fonctionnement des services, les conditions d'utilisation, les processus internes, etc.

En ce qui concerne la question de savoir si les plateformes subiront des conséquences en raison de la diffusion de contenus préjudiciables, comme c'est le cas pour les contenus illégaux, il convient de souligner que, selon le DSA, elles n'auront pas l'obligation de supprimer les contenus préjudiciables, et qu'aucune autorité de contrôle ne pourra le leur demander. Ce n'est que dans l'éventualité où un risque systémique significatif surviendrait concernant plusieurs très grandes plateformes en ligne que la Commission européenne pourrait inviter les plateformes, ainsi que les organisations de la société civile et d'autres parties intéressées, à participer à l'élaboration de codes de conduite qui définiront, entre autres, les obligations de prendre des mesures spécifiques pour réduire les risques, ainsi qu'un cadre pour un reporting régulier de toutes les mesures prises et de leurs effets.

C'est pourquoi un système de responsabilité a été mis en place, comme en témoigne l'exemple du Code de bonnes pratiques en matière de lutte contre la désinformation, qui, d'un simple système d'autorégulation au départ, s’est transformé en un instrument de corégulation. En effet, la Commission européenne a annoncé la signature d'une nouvelle version du Code en 2022, qui sera renforcée par des dispositions plus spécifiques telles que l'obligation de rendre compte plus en détail de l'application du Code à travers des indicateurs clés de performance. L'adhésion au Code ne sera pas contraignante, mais les très grandes plateformes en ligne et les moteurs de recherche

auront de bonnes raisons de le faire afin de respecter leurs obligations en matière d'élimination des risques systémiques. Enfin, en cas de non-exécution des obligations contractées, les sanctions prévues par la législation sur les services numériques, qui constitue à cet égard l'épine dorsale juridique du Code, s'appliqueront.

L'une des dernières modifications apportées à la législation sur les services numériques est la mise en place d'un mécanisme de réponse aux crises, dans le contexte de l'agression russe contre l'Ukraine et de la manipulation de l'information sur internet. Ce mécanisme permet à la Commission européenne d'évaluer l'impact des activités des très grandes plateformes et des moteurs de recherche sur la crise en question, ainsi que de prendre des décisions sur l'application de mesures proportionnées.

3.2.6. Système de reddition de comptes : audit indépendant

Les très grandes plateformes en ligne et les moteurs de recherche devront effectuer un audit annuel indépendant du respect des obligations en vertu de la législation sur les services numériques, y compris l'évaluation des risques et la mise en œuvre de mesures visant à les atténuer. Si un audit indépendant constate que les mesures qu'elles appliquent sont inadéquates, la Commission européenne pourra proposer des corrections et, en fin de compte, imposer des sanctions en cas de non-application.

3.3. Application du DSA

Il ne fait aucun doute que cette législation est un instrument juridique bien conçu, complet et doté d'un grand potentiel, qui établit un équilibre entre un système d'autorégulation et l'établissement de la responsabilité en cas de non-exécution des obligations. Cependant, il convient de souligner une chose importante : comme c'est le cas pour tous les actes législatifs ou réglementaires susceptibles d'avoir un impact fondamental sur une industrie particulière, les effets clés se verront dans la mise en œuvre.

La complexité même des mécanismes envisagé pour réglementer les contenus préjudiciables témoigne de (et démontre) la possibilité de problèmes dans leur application. La grande question est de savoir si l'on peut confier aux plateformes le soin de mener des analyses aussi approfondies et complexes et de décider des meilleurs outils, sachant que c'est précisément la mise en œuvre de cette législation qui est essentielle pour atteindre ses objectifs. Les organisations de la société civile insistent opportunément sur l'application cohérente des règles envisagées, en se référant aux leçons apprises lors de l'application d'une autre législation bien connue (et qui a été copiée autour du monde), le Règlement général sur la protection des données (RGPD), dont l'application a selon les organisations de la société civile largement échoué[22].

[22] https://www.amnesty.org/en/latest/news/2022/04/european-union-digital-services-act-agreement-a-watershed-moment-for-internet-regulation/

Alors que la législation sur les services numériques ne s'appliquera qu'au territoire de l'Union européenne, certains pensent que ses effets se feront sentir « par ricochaet » dans d'autres parties du monde, comme cela été le cas pour le RGPD, car il sera plus rentable pour les entreprises technologiques de mettre en œuvre une stratégie unique et mondiale de modération du contenu. Il reste toutefois à voir si le DSA aura un impact sur les législateurs américains, au niveau fédéral et des Etats, qui ont jusqu'à présent évité de prendre au sérieux la réglementation des grandes entreprises technologiques[23].

[23] https://www.theverge.com/2022/4/23/23036976/eu-digital-services-act-finalized-algorithms-targeted-advertising

4. Initiatives d'autorégulation

Il existe un grand nombre d'alliances et d'initiatives, trop nombreuses et trop variées dans leur approache et leurs objectifs pour être mentionnées ici, qui abordent les questions de protection des mineurs en ligne. Il faut saluer ces efforts multiples et vriés qui reposent sur l'utilisation efficace de ce que les géants du web peuvent offrir en termes de « trouvabilité », d'accessibilité et de notoriété, ce qui agit comme une sorte de « vaccin » contre les perceptions malsaines du monde.

Parmi les exemples notables, citons le fait que la Commission européenne a récemment adopté une nouvelle stratégie européenne pour un meilleur Internet pour les enfants (« Better Internet for Kids + »), afin d'améliorer les services numériques adaptés à l'âge et de veiller à ce que chaque enfant soit protégé, responsabilisé et respecté en ligne, y compris en ce qui concerne les contenus préjudiciables, les dangers d'exposition à la désinformation, le cyberharcèlement, etc.

Cette nouvelle stratégie vise à offrir des contenus et des services en ligne accessibles, adaptés à l'âge et informatifs, qui soient dans l'intérêt supérieur de l'enfant. Tout en veillant à ce que les enfants puissent s'épanouir dans un environnement numérique sûr et stimulant, avec un accès aux appareils et aux compétences numériques, en particulier pour les enfants qui se trouvent dans des situations vulnérables.

La stratégie reconnaît la nécessité de veiller à ce que les enfants jouissent des mêmes droits en ligne et hors ligne, sans qu'aucun enfant ne soit laissé pour compte, quels que soient ses antécédents géographiques, économiques et personnels. Elle établit des normes de sécurité élevées et promeut l'autonomisation des enfants et leur participation active au développement numérique dans le monde entier. Elle prend acte de l'adoption et du respect des normes de la législation sur les services numériques qui, comme nous l'avons mentionné, contient de nouvelles garanties pour la protection des mineurs et interdit aux plateformes en ligne d'afficher des publicités ciblées basées sur le profilage des mineurs.

Les principes et les piliers de cette stratégie définissent la vision d'une décennie numérique pour les enfants et les jeunes, qui repose sur trois piliers clés :

- des expériences numériques sûres, en protégeant les enfants contre les contenus, les comportements et les risques en ligne préjudiciables et illégaux et en améliorant leur bien-être grâce à un environnement numérique sûr et adapté à leur âge ;
- l'autonomisation numérique afin que les enfants acquièrent les aptitudes et les compétences nécessaires pour faire des choix éclairés et s'exprimer dans l'environnement en ligne de manière sûre et responsable ;
- une participation active, en respectant les enfants en leur donnant leur mot à dire dans l'environnement numérique, avec davantage d'activités dirigées par les enfants pour favoriser des expériences numériques sûres innovantes et créatives.

D'ici 2024, la Commission européenne facilitera l'adoption d'un code de l'Union européenne pour la conception adaptée à l'âge et demandera l'adoption d'une norme européenne sur la vérification de l'âge en ligne. Il s'agira également d'examiner la meilleure façon de soutenir le signalement rapide des contenus illégaux et préjudiciables et de veiller à ce que le numéro unique européen « 116 111 » fournisse une assistance aux victimes de cyberharcèlement.

En outre, la Commission européenne organisera des campagnes d'éducation aux médias à l'intention des enfants, des enseignants et des parents, par l'intermédiaire du réseau des centres pour un Internet plus sûr, et proposera des modules d'enseignement aux enseignants via le portail betterinternetforkids.eu. Le réseau des centres pour un internet plus sûr dans les États membres, actif aux niveaux national et local, renforcera le soutien aux enfants en situation de vulnérabilité et contribuera à réduire la fracture numérique en matière de compétences.

Il convient également de noter que la Commission européenne travaille actuellement à l'adoption du code de conduite de l'UE sur la conception adaptée à l'âge (code BIK). Il vise à renforcer l'implication des acteurs de marché dans la protection des enfants lorsqu'ils utilisent des produits numériques, dans le but ultime d'assurer leur vie privée et leur sécurité en ligne. Il s'appuiera sur le cadre réglementaire susmentionné prévu par la législation sur les services numériques et la Directive SMA révisée[24].

Pour terminer ce panorame, et sans qu'il soit possible de détailler ces initiatives ici, il convient de mentionner que dans le cadre de ses projets Global Kids Online[25] et Disrupting Harm[26], l'Unicef recueille des données probantes sur les droits, les opportunités et les risques numériques des enfants afin de mieux comprendre comment l'utilisation de la technologie numérique contribue à leur vie – et quand elle amplifie leur risque de préjudice.

[24] https://digital-strategy.ec.europa.eu/fr/policies/group-age-appropriate-design
[25] http://globalkidsonline.net/
[26] https://www.unicef-irc.org/research/disrupting-harm

5. Conclusion

Il est évident que les récentes initiatives politiques de l'Union européenne s'éloignent des mécanismes purement autorégulateurs de l'industrie, qui ont prévalu depuis les débuts de l'internet, au profit de mesures de corégulation et même de régulation car, au cours de la dernière décennie, l'Europe s'est efforcée de trouver une réponse adéquate au problème croissant de la diffusion de contenus illégaux et préjudiciables dans l'espace en ligne, qui posent des problèmes en matière de vivre-ensemble en général et de protection de l'enfance en particulier.

Alors que les formes les plus extrêmes de contenus illégaux, telles que l'abus et l'exploitation sexuels d'enfants, la pédopornographie et l'incitation au terrorisme, sont réglementées par des lois à l'échelle de l'Union européenne, qui obligent les États membres à appliquer des mesures pour supprimer et bloquer les sites internet contenant ou diffusant ce contenu, l'accès aux discours de haine et aux catégories de contenus légaux mais préjudiciables repose sur des mécanismes d'autorégulation (tels que le code de conduite susmentionné contre les discours de haine illégaux en ligne) qui, cependant, n'a pas produit de résultats adéquats. La question s'est posée de savoir si l'on pouvait vraiment s'attendre à ce que les plateformes en ligne en tant qu'entreprises privées soient responsables de la protection de l'intérêt public sans aucun système de contrôle et de responsabilité, ou si ces problèmes nécessitaient encore un rôle plus important des États et des institutions publiques.

C'est précisément l'absence de réponse adéquate au niveau de l'Union européenne qui a conduit à ce que certains pays aient commencé à réglementer l'espace en ligne avec des lois nationales sans attendre les initiatives européennes, comme ce fut le cas en Allemagne et en France. En plus d'être une réponse nationale à un problème transnational, donc potentiellement dépourvu de sa puissance, ce qui est problématique à propos de ces lois et d'autres lois similaires, ce sont les conséquences négatives qu'elles ont sur la liberté d'expression en encourageant les plateformes à renforcer toutes les normes de la communauté en ligne et à censurer préventivement l'expression valide et légale afin de se prémunir contre toute responsabilité légale, en fonction de chaque pays. Cela a eu pour effet de laisser la réglementation des contenus illégaux et préjudiciables sur internet à des entreprises privées, qui, il ne faut pas l'oublier, sont motivées par des intérêts financiers, au lieu de laisser la réglementation entre les mains d'institutions publiques qui ont l'obligation de travailler dans l'intérêt général. Une telle situation a conduit à une concurrence de fait de la souveraineté entre les États et les entreprises privées. En plus du problème de la modération excessive, il y a aussi le problème de la suppression insuffisante des contenus selon les signalements des utilisateurs. C'est à tous ces problèmes que la législation sur les services numériques tente d'apporter des réponses.

En outre, nous devons tenir compte du fait que la Directive SMA révisée donne explicitement aux autorités de régulation la tâche d'évaluer les préjudices lorsqu'ils décident des niveaux appropriés de mesures de protection à appliquer à la fois par

les fournisseurs de SMA et les fournisseurs de PPV, et d'adopter une approche proportionnée fondée sur une telle évaluation. De plus, les régulateurs devront évaluer la pertinence des mesures prises par les PPV. Sur cette base, les régulateurs seront plus que jamais tenus de comprendre comment les contenus préjudiciables affectent les enfants, et ce qui constitue en fait un contenu préjudiciable, afin d'être en mesure de prendre les mesures appropriées et proportionnées.

C'est particulièrement difficile dans le monde en ligne, où les préjudices potentiels vont bien au-delà de ce que les régulateurs connaissent dans l'environnement médiatique traditionnel : exposition à des contenus générés par les utilisateurs, contacts en ligne inappropriés, cyberintimidation, violation des données personnelles des enfants... En outre, il faut tenir compte du fait que la régulation est relativement « confortable » dans un monde régi par par des responsabilités éditoriales entre les mains de rédactions qui veillent à l'équilibre à un relatif équilibre entre les droits et les responsabilités, mais que le risque devient plus grand lorsque les moyens de protection deviennent en fait mécanisés et automatisés[27].

Le défi consiste donc à trouver un équilibre entre les mesures qui doivent être prises pour protégrer l'intérêt général, en ce compris celui des publics les publics les plus vulnérables comme les mineurs, et les avantages et les opportunités que l'utilisation d'internet apporte aux mineurs.

Un autre défi sera l'interaction inévitable entre les nombreux acteurs et parties prenantes qui partagent la responsabilité de la protection des mineurs dans le monde en ligne, tels que les organismes gouvernementaux, les tribunaux, d'autres autorités de régulation telles que les organismes de télécommunications et de protection des données, les organismes de recherche, la société civile et les associations de consommateurs, ainsi que les acteurs du secteur des médias.

C'est précisément en raison de ces circonstances contemporaines difficiles qu'il est nécessaire, aujourd'hui plus que jamais, de faire tout ce qui est possible pour protéger les mineurs. Tout d'abord, il est encore trop tôt pour évaluer et parler des effets de certains des instruments juridiques susmentionnés. Ce que l'on remarque dans les approches présentées en matière de régulation des contenus en ligne préjudiciables, c'est la mise en place de plateformes de coopération entre des institutions et des acteurs qui ont des compétences et des rôles différents dans l'environnement numérique, compte tenu de l'ampleur et de la diversité des domaines en question. Le mécanisme de mise en œuvre des obligations découlant de la législation sur les services numériques, par exemple, devrait donc, au lieu d'une approche centralisée, reposer sur une coopération et une coordination intersectorielles entre les institutions responsables des communications électroniques et des médias, de la protection des données personnelles, de la sauvegarde de la concurrence, de la protection des consommateurs, … avec le soutien des universités et des organisations de la société civile. La priorité devrait être donnée à des structures de coopération intersectorielles,

27 https://cdn.epra.org/attachments/files/3616/original/Bakground_paper_plenary_1_v29102019_WM.pdf?1572425159

qui ne sont pas là pour protéger les intérêts particuliers de qui que ce soit, mais les intérêts collectifs de tous. L'un des problèmes est que de telles structures nécessitent la coopération d'acteurs très différents, ce qui nécessite de la flexibilité et de l'adaptabilité, mais aussi de trouver plus que jamais un équilibre entre l'intensification de la coopération et la préservation de l'indépendance de chacune des parties prenantes.

Il y a une dernière chose à considérer. Selon Oxford University Press, qui publie l'Oxford English Dictionary, le mot gagnant pour 2022, pour la première fois sélectionné pour être ajouté au dictionnaire par un vote populaire, est *« mode gobelin »*, un terme d'argot décrivant un comportement *« sans vergogne complaisant, paresseux, négligé ou avide »*[28]. Un type de comportement qui est sans vergogne complaisant, paresseux, négligent ou avide, généralement d'une manière qui rejette les normes ou les attentes sociales, résonne comme une réaction adéquate à l'état du monde. On peut voir la parentalité permissive prendre lentement le pas sur les normes précédemment établies. Abusés par leurs parents, couplés à l'individualisme et à l'aliénation inévitables qui peuvent découler d'une présence excessive en ligne, de plus en plus de mineurs présentent les caractéristiques de personnes autocentrées ou narcissiques. Parmi les causes, citons l'incapacité des parents à faire respecter des limites cohérentes et adaptées à l'âge, les parents qui protègent l'enfant des frustrations quotidiennes normales, l'octroi de cadeaux matériels excessifs, même lorsque l'enfant ne s'est pas comporté de manière appropriée, et la fourniture de modèles inappropriés.

Les modèles, en particulier ceux qui ne sont pas appropriés, ont été détaillés ici. En ce sens, nous devons noter que les circonstances actuelles dans le monde sont pour le moins sombres. Les guerres font rage, des enfants sont tués quotidiennement, les famines se propagent, les effets du changement climatique sont indéniables et, dans certaines parties du monde, déjà catastrophiques. De plus, des dangers et des préjudices se cachent à chaque coin d'internet pour les mineurs. Le contenu violent et agressif est omniprésent, à tel point que même l'amour semble corrompu par des vampires et des zombies. Le danger fondamental de l'exposition des enfants à des préjudices et à la violence est qu'elle augmente leur niveau d'acceptation de ces formes de comportement inacceptables, en les copiant et en les adoptant comme « normales », ou tout à fait acceptables, voire justifiées dans un contexte historique et culturel donné.

Dans toutes ces circonstances, nous ne pouvons pas nous attendre à ce que les enfants s'écartent beaucoup des modèles de comportement fournis autour d'eux par les adultes. En effet, les enfants sont exposés à de nombreux dangers en ligne, mais nous devons accepter que le monde réel ne leur fournit pas de filets de sécurité, de normes de comportement basées sur la tolérance, la responsabilité, le respect, la considération ou l'empathie.

[28] https://languages.oup.com/word-of-the-year/2022/

C'est donc la conclusion de cette étude : il faut faire tout ce qui est possible, à partir des initiatives législatives et d'autorégulation susmentionnées, pour assurer la sécurité de nos enfants en ligne, mais nous ne devons pas oublier que nos enfants vivent dans le monde actuel, à commencer par la famille, ce noyau de base qui transforme les enfants en adultes et qui fournit la source principale des normes et des standards de comportement. Mis en ligne avec une portée et une disponibilité sans précédent, le comportement des êtres humains d'aujourd'hui est un modèle de comportement pour nos enfants, et il est grand temps que notre société réexamine fondamentalement la situation dans ce contexte. S'il n'est pas déjà trop tard.