PANTHÉON-ASSAS
UNIVERSITÉ
PARIS

**BANQUE DES MÉMOIRES**

**Master de Droit du numérique**
**Dirigé par Monsieur le Professeur Jérôme PASSA**
**2023-2024**

# *La souveraineté numérique à l'épreuve du libre accès aux sites pornographiques*

**Réjane GAONAC'H**

**Sous la direction de Maître Ilène CHOUKRI**

*Les opinions exprimées dans ce mémoire sont propres à leur auteur et n'engagent pas l'Université Paris Panthéon-Assas.*

# *Remerciements*

La rédaction de ce mémoire a été possible grâce au concours de quelques personnes auxquelles je souhaite témoigner ma reconnaissance.

Mes remerciements s'adressent d'abord à Maître Ilène Choukri, ma directrice de mémoire, pour sa bienveillance, ses propositions et ses judicieux conseils, lesquels m'ont permis d'appréhender la profondeur du sujet et ses enjeux primordiaux.

À Monsieur le Professeur Olivier Blazy, que je remercie sincèrement pour sa gentillesse, pour le temps qu'il a accordé à notre entretien et pour la clarté de ses réponses.

J'adresse bien sûr mes remerciements à Emma, Manon et Ismail pour leur disponibilité et leur aide précieuse à la relecture de ce mémoire.

Je souhaite exprimer enfin ma sincère reconnaissance à Aurélien, pour m'avoir partagé sa passion de l'informatique, pour son expertise sur des notions clés de ce mémoire, mais surtout pour son soutien indispensable et indéfectible.

## *Principales abréviations*

| | |
|---|---|
| **ANSSI** | Agence nationale de la sécurité des systèmes d'information |
| **Arcom** | Autorité de Régulation de la Communication Audiovisuelle et Numérique |
| **CEDH** | Cour européenne des droits de l'Homme |
| **CJUE** | Cour de justice de l'Union européenne |
| **CNIL** | Commission Nationale de l'Informatique et des Libertés |
| **ConvEDH** | Convention européenne des droits de l'Homme |
| **CSA** | Conseil Supérieur de l'Audiovisuel |
| **DNS** | Domain Name System |
| **DSA** | Digital Services Act |
| **FRA** | Agence des droits fondamentaux de l'Union européenne |
| **LINC** | Laboratoire d'innovation numérique de la CNIL |
| **Loi LCEN** | Loi pour la confiance dans l'économie numérique |
| **Loi SREN** | Loi visant à sécuriser et réguler l'espace numérique |
| **OCLCTIC** | Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication |
| **OFCOM** | Office of Communications |
| **ONU** | Organisation des Nations unies |
| **PEReN** | Pôle d'expertise de la régulation numérique |
| **RGPD** | Règlement général sur la protection des données |
| **SGIN** | Service de garantie de l'identité numérique |
| **UE** | Union européenne |
| **VPN** | Réseau privé virtuel |

# *Table des matières*

**Introduction** ..... 2

**I. Une vérification de l'âge respectueuse de la vie privée des visiteurs de sites pornographiques** ..... 7

***A. L'émission d'une preuve de l'âge conforme aux exigences légales et règlementaires*** ..... ***7***

*1. Les contraintes de l'estimation algorithmique de l'âge à l'état de l'art* ..... 7

*2. L'encadrement du contrôle de l'âge en tant qu'attribut de l'identité* ..... 13

***B. La transmission de la preuve de l'âge protégée par le dispositif de «double anonymat»*** ..... ***17***

*1. La garantie de fiabilité du protocole zero-knowledge proof* ..... 17

*2. La garantie de confidentialité du tiers vérificateur* ..... 22

**II. La maîtrise du blocage étatique de l'accès aux sites pornographiques** ..... 27

***A. Les difficultés de restriction territoriale de l'accès aux sites pornographiques*** ..... ***27***

*1. Les incertitudes juridiques relatives au déréférencement et au blocage des sites* ..... 27

*2. L'accessibilité aux outils de contournement du géoblocage* ..... 32

***B. Les perspectives de nationalisation d'Internet*** ..... ***36***

*1. Le déploiement d'un réseau étatique centralisé* ..... 36

*2. Les risques de censure de la liberté d'expression* ..... 41

**Conclusion** ..... 47

**Annexes** ..... 50

***Annexe 1*** ..... ***50***

***Annexe 2*** ..... ***56***

**Bibliographie** ..... 57

## Introduction

*« En 2023, c'est la fin de l'accès aux sites pornographiques pour nos enfants ! »*[1]. Lors d'une audition devant la délégation aux droits des enfants, le ministre chargé du Numérique, Jean-Noël Barrot, réaffirmait la volonté du gouvernement à imposer aux sites pour adultes une vérification effective de l'âge des internautes. Force est de constater qu'aujourd'hui, il suffit toujours d'un clic pour répondre positivement à la question *« Avez-vous 18 ans ? »* et ainsi accéder à la majorité des contenus interdits aux mineurs. Une étude récente[2] de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) révèle que le nombre de mineurs visitant des sites pornographiques chaque mois a augmenté de 36% en 5 ans, alors même que le nombre d'adultes est resté stable. L'étude souligne également la précocité de ce phénomène ; dès 12 ans, plus de la moitié des garçons se rendent sur ces sites au moins une fois par mois. Au-delà des considérations morales, éthiques ou religieuses, ces chiffres inquiètent par leur impact sur la sexualité des jeunes Français[3], et motivent l'adoption de mesures contraignantes visant à limiter l'accès des mineurs aux contenus à caractère sexuel sur Internet.

**Régulation de l'accès aux sites pornographiques en France.** Le législateur a adopté la loi du 30 juillet 2020[4] en vue d'imposer une vérification de l'âge à l'entrée des sites pornographiques accessibles en France. Les modalités de cette vérification ont été précisées dans un décret du 7 octobre 2021[5], permettant au Conseil Supérieur de l'Audiovisuel (CSA), devenu l'Arcom, de saisir le tribunal judiciaire pour bloquer l'accès aux sites refusant de se soustraire à cette exigence de vérification. Or, la mise en application de ces mesures a révélé les limites d'une telle régulation : les dispositifs de vérification de l'âge ont été jugés soit insuffisamment fiables, soit, au contraire, attentatoires aux libertés individuelles. En réponse à ces difficultés, le gouvernement français a consolidé son arsenal législatif avec la loi visant à sécuriser et réguler l'espace numérique (loi SREN) publiée au Journal officiel le 22 mai 2024. La loi prévoit l'élaboration d'un référentiel technique commun de l'Arcom et de la Commission Nationale de l'Informatique et des Libertés (CNIL) précisant les exigences en matière de

[1] Anonyme. (2023). Sites pornos : le système de vérification d'âge du gouvernement testé en mars. *Le Parisien avec AFP.* https://www.leparisien.fr/societe/sites-pornos-le-systeme-de-verification-dage-du-gouvernement-teste-en-mars-14-02-2023-PD6YYMDSJJDRZEPFJPQ7BAQFZQ.php.

[2] Arcom. (2023). Fréquentation des sites adultes par les mineurs. https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs.

[3] Smaniotto, B. (2023). Pornographie : quels impacts sur la sexualité adolescente ? *The Conversation*. https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142.

[4] Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

[5] Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

protection des données personnelles pour les outils de contrôle de la majorité. La force obligatoire de ce référentiel repose notamment sur les prérogatives accordées à l'Arcom : celle-ci aura désormais le pouvoir d'ordonner le blocage et le déréférencement des sites ne se conformant pas aux normes établies dans son référentiel, et ce, sans l'intervention du juge judiciaire. Cette initiative reflète la volonté de l'État français de garantir un blocage rapide de l'accès à ces sites, et ainsi assurer un contrôle plus efficace de l'espace numérique national.

**Définition de la souveraineté numérique.** L'encadrement étatique de ce contrôle prend appui sur le concept de souveraineté numérique, défini dans un rapport de la commission d'enquête du Sénat[6] comme *« la capacité de l'État à agir dans le cyberespace »*. Le rapport précise que l'exercice de cette souveraineté repose sur la *« capacité autonome d'appréciation, de décision et d'action dans le cyberespace »*, mais également sur la maîtrise de *« nos réseaux, nos communications électroniques et nos données »*. En ce sens, la capacité d'un État à imposer ses lois dans l'espace numérique constitue l'un des enjeux contemporains de l'exercice de la souveraineté numérique. Parallèlement à l'action des États, cette souveraineté s'exerce à l'échelle de l'Union européenne (UE), notamment par l'adoption de règles encadrant la protection des données face aux lois extraterritoriales[7] et la création de nouvelles obligations visant à responsabiliser les acteurs du numérique[8]. À ce titre, la politique européenne du numérique peut aider à consolider la souveraineté numérique des États membres. Dans son discours sur l'état de l'Union du 16 septembre 2020, la présidente de la Commission européenne, Ursula von der Leyen, consacrait d'ailleurs le renforcement de la souveraineté numérique en tant qu'enjeu de l'UE[9]. Toutefois, cette approche communautaire ne doit pas nier la souveraineté nationale dans sa conception « physique » du territoire ; en effet, l'exercice de la souveraineté est intrinsèquement relié à l'État, et à son pouvoir d'agir sur un territoire donné. Ainsi, en matière numérique, une articulation doit être trouvée entre l'affirmation de la souveraineté européenne, et celle de la souveraineté nationale. Si l'UE a récemment imposé des règles renforcées à trois grandes plateformes hébergeant des contenus pornographiques dans le cadre sa nouvelle loi sur les services numériques[10], la protection des mineurs face aux images

[6] Sénat. (2019). Le devoir de souveraineté numérique. Rapport n° 7 (2019-2020), tome I. https://www.senat.fr/rap/r19-007-1/r19-007-1_mono.html.
[7] Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[8] Règlement 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.
[9] Commission européenne. (2020). Discours sur l'état de l'Union de la présidente von der Leyen en session plénière du Parlement européen. https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_20_1655.
[10] Commission européenne. (2023). La Commission désigne une deuxième série de très grandes plateformes en ligne au titre du règlement sur les services numériques. https://ec.europa.eu/commission/presscorner/detail/fr/IP_23_6763.

à caractère sexuel constitue un enjeu de santé publique qui relève de la compétence des États membres. En principe, ceux-ci peuvent donc adopter des mesures de contrôle de l'accès aux sites pornographiques visant à s'appliquer sur leur territoire national.

**Définition du cyberespace**. La capacité d'un État à agir sur son territoire doit être distinguée de sa capacité à agir dans le cyberespace ; d'abord parce qu'il n'existe pas de définition communément admise du cyberespace, dans la mesure où il s'agit d'un concept relativement récent[11]. La Professeure des Universités et membre de la Global Commission on the Stability of Cyberspace, Frédérick Douzet, en propose une définition *« a minima »* : le cyberespace renverrait à la fois à Internet et à *« l'espace qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance »*[12]. Le cyberespace revêt ainsi une nature transfrontière, et il n'existe pas d'instance supranationale destinée à la coopération des États en matière de régulation de l'Internet[13]. En conséquence, chaque État revendique le prolongement de son pouvoir de réglementation dans le cyberespace, et les lois nationales se superposent. L'existence d'un cyberespace « national » impliquerait pour un État de maîtriser les flux transitant sur les différentes couches composant le cyberespace, tel qu'explicité par le stratégiste et géopolitologue Olivier Kempf ; ces couches *« peuvent être physiques (dorsales sous-marines ou terrestres, points d'échanges Internet, fermes de données centrales…), logiques (maîtrise des principaux logiciels d'exploitation, antivirus nationaux, nuages souverains) ou sémantiques (inculturation des pratiques d'Internet nationales, utilisation de la langue ou de l'alphabet, utilisation de réseaux sociaux d'inspiration nationale) »*[14]. Or, cette aspiration se heurte à la réalité de la mondialisation numérique, où les flux transfrontaliers sont omniprésents et défient les tentatives de contrôle des États.

**Blocage de l'accès aux sites pornographiques.** Bien qu'aucun État ne puisse prétendre maîtriser l'ensemble des flux transitant dans le cyberespace, le blocage de l'accès à certains sites est un phénomène répandu et constitue l'un des principaux modes de régulation de l'Internet. La notion de blocage a été définie par le Rapporteur spécial des Nations unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, dans

[11] La notion de cyberespace, introduite par le romancier William Gibson dans les années 1980, n'a commencé à prendre une dimension politique et géopolitique qu'à la fin des années 1990. Source : https://doi.org/10.3917/her.152.0003.
[12] Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote*, 152-153, 3-21. https://doi.org/10.3917/her.152.0003.
[13] Ibid.
[14] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions*, 30, 141-149. https://doi.org/10.3917/infle.030.0141.

son rapport de mai 2011, comme une série de *« mesures prises pour empêcher un utilisateur final d'avoir accès à certains contenus »*[15], mesures qui consistent à *« empêcher les utilisateurs d'accéder à certains sites Web, aux adresses de protocole Internet (IP), aux extensions de nom de domaine »*[16]. Parmi les motifs de blocage, figurent notamment la censure du débat politique, la censure relative à la lutte contre la criminalité (vente d'armes, pédopornographie…) ou encore la censure dans un intérêt de protection de la sécurité nationale. En ce qu'il s'agit spécifiquement des sites pour adultes, la plupart des gouvernements ayant établi une large censure du Web interdisent également la pornographie ; c'est le cas de l'Ouzbékistan, du Qatar, de l'Arabie saoudite ou encore de la Chine, où de nombreux sites jugés illicites voire « immoraux » sont bloqués[17]. En Islande, un projet ambitieux d'interdiction de la pornographie en ligne, proposé en 2013 par le ministre de l'Intérieur, a finalement été abandonné en raison des préoccupations liées à la liberté d'expression[18].

**Filtrage des mineurs à l'entrée des sites pornographiques.** Au regard des contraintes technico-légales du blocage, certains États démocratiques ont tenté de limiter l'accès aux sites pornographiques aux seules personnes mineures ; dès 1996, les États-Unis adoptaient le *Communications Decency Act*, prévoyant l'interdiction de la diffusion de contenus à caractère sexuel aux mineurs sur Internet. Cette loi fut toutefois partiellement invalidée par la Cour suprême, en raison des risques d'atteinte à la liberté d'expression[19]. D'autres tentatives de règlementation, plus récentes, ont également été abandonnées ; en Australie par exemple, les autorités ont tenté de mettre en place un système de vérification de l'âge similaire à celui encadré par la loi SREN en France, mais le gouvernement a renoncé à ce projet, en raison de la fiabilité insuffisante des outils de vérification, et des inquiétudes quant au respect de la vie privée[20]. Ainsi, les initiatives des États aboutissent au même constat : l'objectif de protection des mineurs face au libre accès aux sites pornographiques se heurte à des droits et libertés essentiels au fonctionnement des sociétés démocratiques.

---

[15] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[16] Ibid.

[17] Leloup, D., Untersinger, M., & Reynaud, F. (2015). L'impossible censure des sites pornographiques. *Le Monde*. https://www.lemonde.fr/pixels/article/2015/08/04/une-breve-histoire-de-la-censure-des-sites-pornographiques_4711451_4408996.html.

[18] Ibid.

[19] Leary, MG. (2022). *§230 of the Communications Decency Act: Regarding Child Sexual Abuse Material - The Experiment is Done and it Failed.* CUA Columbus School of Law Legal Studies. https://ssrn.com/abstract=4254010.

[20] Anonyme. (2023). Sites pornographiques : l'Australie abandonne son projet de vérification de l'âge des internautes. *Le Monde*. https://bit.ly/3yKztAJ.

**Intérêt et délimitation du sujet.** Le présent mémoire a pour intérêt d'étudier les nombreux enjeux relatifs à la régulation de l'accès aux sites pornographiques. Il vise à mettre en lumière les difficultés rencontrées par les États à imposer une vérification efficace de l'âge des internautes et à procéder au blocage des sites offrant un accès libre à leurs contenus. En outre, il s'agira d'établir une corrélation entre l'effectivité des mesures visant à restreindre cet accès, et l'affirmation de la souveraineté numérique de l'État régulateur, au regard de sa capacité à imposer le respect de ses lois dans le cyberespace. Il convient de préciser que ce mémoire n'a pas vocation à proposer une définition exhaustive de la pornographie. Cet écueil présente toutefois l'intérêt d'approcher la complexité du sujet en évitant toute interprétation erronée ou stéréotypée. Sur ce point, le Parlement européen a justement relevé que *« toute tentative sérieuse de définition met en lumière le caractère éminemment relatif, subjectif et évolutif de ce qui peut être considéré comme pornographie »*[21]. Cependant, à des fins de délimitation adéquate du sujet, ce mémoire portera uniquement sur les sites dont la fonction principale est d'héberger des contenus à caractère pornographique, excluant de fait les contenus accessibles sur les réseaux sociaux. Il s'agira, enfin, de proposer une analyse du sujet basée sur l'ambition française de régulation de l'accès aux sites pornographiques, illustrée par la loi SREN récemment adoptée. Une approche comparative s'imposera pour inclure des exemples pertinents de régulations mises en œuvre par des gouvernements étrangers.

Au regard de ce qui a été exposé, ce mémoire adressera la problématique suivante :

**En quoi la lutte contre l'accès illégal des mineurs aux sites pornographiques révèle-t-elle la capacité d'un État à exercer sa souveraineté numérique ?**

L'exercice de la souveraineté numérique dans la régulation de l'accès aux sites pornographiques s'envisage principalement par le biais d'un double contrôle. Le prérequis fondamental est celui d'un filtrage efficace des mineurs à l'entrée des sites pornographiques, mais cette vérification de l'âge doit impérativement garantir la protection de la vie privée des internautes (I). Lorsque l'éditeur d'un site ne se conforme pas à l'exigence légale de vérification, l'État régulateur doit être capable d'en bloquer tout accès émanant de son territoire, mais également de justifier cette censure arbitraire (II).

[21] Parlement européen. (1993). Rapport de la commission des libertés publiques et des affaires intérieures sur la pornographie, PE 204.502/déf.

## I. Une vérification de l'âge respectueuse de la vie privée des visiteurs de sites pornographiques

Le 5 janvier 2023, la Cour de cassation s'est saisie d'une question prioritaire de constitutionnalité sur le dispositif de vérification de l'âge prévu par la loi du 30 juillet 2020, et a déclaré que : *« l'atteinte portée à la liberté d'expression, en imposant de recourir à un dispositif de vérification de l'âge de la personne accédant à un contenu pornographique, autre qu'une simple déclaration de majorité, est nécessaire, adaptée et proportionnée à l'objectif de protection des mineurs »*[22]. Cette vérification implique, à l'évidence, un traitement de données, qui peut être mis en relation avec des informations intimes ; il est donc essentiel d'adopter une méthode de vérification de l'âge fiable et non-intrusive (A). La preuve de majorité doit ensuite être transmise de façon confidentielle pour garantir aux utilisateurs la protection de leur anonymat (B).

### *A. L'émission d'une preuve de l'âge conforme aux exigences légales et règlementaires*

En vue de distinguer les personnes mineures des personnes majeures lors des tentatives d'accès aux sites pornographiques, une question préalable se pose : faut-il estimer l'âge de l'individu ou procéder à une vérification de son identité ? Dans les deux cas, le choix de la méthode envisagée est limité par l'existence de normes internes et supranationales qui encadrent rigoureusement l'utilisation d'algorithmes (1) et le contrôle de l'âge sur la base de documents révélant l'identité de l'utilisateur (2).

#### *1. Les contraintes de l'estimation algorithmique de l'âge à l'état de l'art*

**Intérêt de l'usage des solutions algorithmiques.** À l'entrée en vigueur de la loi de 2020, de nombreuses plateformes hébergeant des contenus pornographiques ont tenté de mettre en place une vérification de l'âge respectueuse de l'anonymat de leurs utilisateurs. Néanmoins, en l'absence d'outils adaptés, la plupart ont limité ce contrôle à la déclaration de majorité par le biais d'un simple clic, voire de l'entrée manuelle de la date de naissance par l'utilisateur lui-même ; d'autres ont choisi de recourir à des algorithmes d'intelligence artificielle pour effectuer

[22] Cass. 1re civ., 5 janv. 2023, n° 22-40.017 : JurisData n° 2023-000021 ; Dalloz actualité, 19 janv. 2023, obs. J. Groffe-Charrier.

une estimation de l'âge. Au regard des garanties de confidentialité, les méthodes d'estimation de l'âge présentent un intérêt certain, puisqu'elles consistent à présumer l'âge d'un individu sans l'identifier[23]. Cette estimation peut s'opérer, par exemple, par le biais de l'analyse de la « maturité » de l'utilisateur sur la base d'un questionnaire (ce qui éviterait tout transfert de données personnelles) ou par l'analyse de ses données de navigation sur les services propres à l'éditeur du site (si aucune donnée supplémentaire n'est collectée). Toutefois, le degré de précision de ces estimations est déterminant au regard de leur fiabilité ; elles peuvent donc être perçues comme étant insuffisamment efficaces. L'analyse faciale, quant à elle, permet d'estimer l'âge d'un individu sans l'identifier précisément. Cette solution se distingue de la reconnaissance faciale, puisqu'elle n'implique pas l'analyse de données biométriques[24], définies comme *« les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques [empreintes digitales] »*[25]. Ainsi, la distinction entre « analyse » et « reconnaissance » faciale est essentielle dans la mise en œuvre des solutions de vérification d'âge, car les deux technologies reposent sur des principes similaires de vision par ordinateur et de traitement d'image. La CNIL s'est d'ailleurs prononcée en défaveur de l'utilisation d'outils de reconnaissance faciale, déclarant que *« les procédés techniques visant à vérifier la majorité d'âge ne sauraient conduire au traitement de données biométriques au sens de l'article 9 du RGPD »*[26], notamment en raison de la nature sensible de ces données. L'autorité a ensuite précisé sa position, en admettant la validité des procédés d'estimation de l'âge *« reposant sur une analyse faciale sans reconnaissance faciale »*[27]. Ainsi, les solutions d'analyse faciale peuvent être utilisées dans le cadre de la vérification de l'âge

[23] CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

[24] CNIL. (2022). Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée. https://www.cnil.fr/fr/controle-de-lage-sur-les-sites-web-la-cnil-invite-developper-des-solutions-plus-efficaces-et.

[25] Article 3, paragraphe 13, de la directive en matière de protection des données dans le domaine répressif ; article 4, paragraphe 14, du RGPD ; article 3, paragraphe 18, du règlement (UE) 2018/1725.

[26] CNIL. (2021). Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

[27] CNIL. (2022). Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée. https://www.cnil.fr/fr/controle-de-lage-sur-les-sites-web-la-cnil-invite-developper-des-solutions-plus-efficaces-et.

prévue par la loi SREN, et de plus en plus d'acteurs économiques se positionnent sur ce nouveau marché[28]. Il convient donc d'appréhender les contours de l'analyse faciale à l'état de l'art.

**Limites techniques de l'analyse faciale.** D'un point de vue technique, la fiabilité des algorithmes d'analyse faciale est débattue à plusieurs égards. D'abord puisqu'il s'agit d'une technologie qui n'est pas infaillible, et qui, à ce titre, présente certaines lacunes ; un rapport du National Institute of Standards and Technology publié en 2018 a révélé, à l'issue d'une comparaison entre 127 algorithmes d'analyse de visages, que le taux de confiance de l'analyse était insuffisamment élevé pour au moins 10% des images[29]. Plus récemment, la start-up britannique Yoti a développé un outil d'analyse faciale pour estimer l'âge des individus, et a estimé l'amplitude de la marge d'erreur à environ 1,6 ans[30], ce qui peut s'avérer insuffisamment précis pour les personnes proches de l'âge de 18 ans. Les systèmes d'analyse faciale doivent également inclure des facteurs tels que la modification de l'apparence (à l'aide de maquillage par exemple), l'éclairage, la ressemblance des visages, etc., qui complexifient l'interprétation du taux d'erreur. Par ailleurs, ces algorithmes doivent être capables de prendre en compte les changements physiques liés à l'âge ainsi que les facteurs susceptibles de les accélérer (comme la consommation de médicaments ou de drogues) ou de les ralentir (comme la chirurgie esthétique). Enfin, ces technologies peuvent intégrer des biais discriminatoires dans leurs algorithmes, se traduisant notamment par un faible taux d'erreur dans l'estimation du sexe des hommes à peau claire, et un taux d'erreur plus élevé dans l'estimation du sexe des femmes à peau foncée[31]. Cela s'explique par l'apprentissage des modèles d'intelligence artificielle, prenant appui sur des bases de données publiques provenant d'images sur Internet, lesquelles ne sont pas forcément représentatives de la diversité physionomique de la population. Ainsi, en dépit des progrès technologiques, les dispositifs d'analyse faciale demeurent imparfaits, insuffisamment fiables, et sont susceptibles de présenter des biais discriminatoires. En outre, l'activation d'une caméra pour procéder à l'analyse faciale des utilisateurs de sites pornographiques pourrait constituer une nouvelle opportunité de « chantage à la webcam » ; il s'agit d'un type d'escroquerie, également appelée « cryptoporno », où un cybercriminel prétend

[28] On peut citer la solution AgeID développée par MindGeek, également propriétaire de plusieurs sites pornographiques, ou encore Yoti, une entreprise britannique dont la solution repose sur l'estimation de l'âge à partir d'une courte vidéo ou photo de l'utilisateur.

[29] Grother, P., Ngan, M. & Hanaoka, K. (2018). Ongoing Face Recognition Vendor Test, part 1., National Institute of Standards and Technology. https://www.congress.gov/116/meeting/house/109578/documents/HHRG-116-GO00-20190604-SD008.pdf.

[30] Anonyme. (2023). Pour contrôler l'âge des joueurs, la FDJ teste un système de reconnaissance faciale. Ouest France. https://bit.ly/4aPHzWg

[31] Buolamwini, J., Gebru, T. (2018). Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91.

avoir piraté l'ordinateur de la victime pour enregistrer des vidéos compromettantes via sa webcam, et menace de les publier si l'utilisateur ne paye pas une rançon en monnaie virtuelle[32]. En ce sens, l'utilisation de l'analyse faciale à l'entrée des sites pornographiques peut être perçue comme une intrusion majeure dans la vie privée des utilisateurs.

**Analyse faciale et droit de l'UE.** En raison de leur nature, les images faciales relèvent de catégories particulières de données à caractère personnel, c'est-à-dire, des données sensibles. À ce titre, la législation de l'UE sur la protection des données prévoit une protection renforcée et des garanties supplémentaires par rapport aux autres données à caractère personnel. Pour déterminer leur niveau de protection, le considérant 51 du Règlement général sur la protection des données (RGPD) distingue la nature juridique des simples « photographies » de celle des « images faciales » biométriques ; ainsi, la définition des données biométriques s'applique aux photographies uniquement lorsque celles-ci *« sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique »*[33]. En vertu de l'article 9, paragraphe 2, point g) du RGPD, le traitement des données biométriques est autorisé uniquement si ce traitement est *« nécessaire pour des motifs d'intérêt public important »* et repose sur le droit de l'Union ou le droit d'un État membre. Dans le cadre de la vérification de l'âge, l'outil d'analyse faciale ne doit en aucun cas permettre d'identifier la personne physique. Toutefois, il est intéressant de relever que l'agence des droits fondamentaux de l'Union européenne (FRA) définit la reconnaissance faciale comme *« le traitement automatique d'images numériques qui contiennent le visage de personnes à des fins d'identification, d'authentification/de vérification ou de catégorisation de ces personnes »*[34]. Cette approche recouvre une multitude de technologies dont les finalités d'utilisation doivent être distinguées ; la vérification et l'identification consistent à déterminer l'identité d'une personne physique, ce qui revient à l'identifier de manière individuelle. La catégorisation, en revanche, permet de déduire l'appartenance d'une personne à un groupe spécifique, sur la base de ses caractéristiques physiques[35]. Cette dernière finalité peut être assimilée à l'analyse faciale dans le cadre de l'estimation de l'âge, qui consisterait, par exemple, à comparer une capture

[32] Cybermalveillance.gouv. (2020). Chantage à la webcam ou à l'ordinateur prétendus piratés, que faire ? https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/chantage-a-lordinateur-ou-a-la-webcam-pretendus-pirates.

[33] Considérant 51 du RGPD.

[34] Groupe de travail « article 29 » sur la protection des données. (2012). Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles », 00727/12/EN, WP 192, page 2. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_fr.pdf.

[35] European Union Agency for Fundamental Rights. (2022). Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi, page 8. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_fr.pdf.

photo ou vidéo de l'utilisateur avec des bases de données contenant des millions visages d'âges variés. Ainsi, même si elle ne permet pas l'identification de la personne, il convient d'encadrer strictement l'utilisation de la « simple » analyse faciale afin d'éviter tout croisement de données. En effet, les caractéristiques d'un visage peuvent potentiellement être liées à d'autres informations personnelles, par exemple les données de localisation, rendant possible l'identification de l'individu[36]. Par ailleurs, les solutions mises en place par les services diffusant des contenus pornographiques ne doivent pas entraîner de discrimination envers certains groupes de population, en particulier pour les motifs énoncés à l'article 21 de la Charte des droits fondamentaux de l'UE. Or, les algorithmes d'analyse faciale sont susceptibles d'intégrer des biais discriminatoires. Il revient donc aux États membres d'adopter des solutions de vérification de l'âge conformes à l'état de l'art et aux standards fixés par le législateur européen.

**Position britannique sur l'analyse faciale.** L'analyse faciale fait partie des méthodes de vérification de l'âge répertoriées par l'Office of Communications (OFCOM), l'autorité de régulation britannique. En octobre 2023, le Royaume-Uni a adopté l'*Online Safety Act* (OSA), fixant des objectifs de protection des mineurs similaires à ceux portés par la loi SREN en France. Dans ses lignes directrices du 5 décembre 2023, l'OFCOM a précisé que l'estimation de l'âge basée sur l'analyse faciale pouvait être une méthode de vérification « hautement efficace » à condition d'être correctement mise en œuvre[37]. En réponse à ces lignes directrices, l'OSA Network a publié une note dans laquelle elle précise que l'expression de « reconnaissance faciale » constitue un abus de langage, puisque la solution agréée n'implique aucune identification[38]. En ce sens, la distinction entre analyse et reconnaissance faciale est primordiale, et doit être précisée en vue de fournir des garanties adéquates au regard des droits fondamentaux. Pour l'instant néanmoins, l'OFCOM ne s'est pas prononcée sur les garanties spécifiques que doivent intégrer les outils de vérification d'âge, considérant qu'il était nécessaire de permettre l'innovation dans ce secteur[39]. Il existe pourtant des standards

[36] European Union Agency for Fundamental Rights. (2022). Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi, page 8. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_fr.pdf.

[37] OFCOM. (2023). Guidance for service providers publishing pornographic content, page 17. https://www.ofcom.org.uk/__data/assets/pdf_file/0017/272600/consultation-part-5-guidance.pdf.

[38] Walsh, M. & Woods, L. (2024). Response to Ofcom's consultation on guidance for providers publishing pornographic content. *Online Safety Act Network*. https://www.onlinesafetyact.net/analysis/response-to-ofcom-s-guidance-for-providers-publishing-pornographic-content/ : *« The method referred to as "face-recognition biometrics" is mis-named. There is no recognition involved (except if that is used later for the purpose of authenticating the user and the same individual who has previously been age verified). This should be renamed "Facial age estimation" ».*

[39] OFCOM, op. cit.. : *« We also want to allow space for important innovation in the safety tech sector. For these reasons, we are not proposing specific metrics that the age assurance process should achieve for each of the criteria».*

britanniques dédiés à l'utilisation de cette solution, tels que le standard PAS 1296:2018 qui définit des « niveaux de certitude » basés sur des « vecteurs de confiance » pour les dispositifs d'estimation de l'âge via analyse faciale[40]. D'ailleurs, en 2017, le projet de loi britannique prévoyait déjà la mise en place d'un système obligatoire de contrôle de l'âge, mais l'avait finalement écarté en raison des limites techniques des méthodes de vérification, et notamment de l'analyse faciale[41]. Si le projet de loi a depuis été modifié, il ne prévoit pas davantage de garanties quant à la fiabilité de cette solution. Néanmoins, cette lacune n'est pas entachée d'illégalité au regard du RGPD, dans la mesure où le retrait du Royaume-Uni de l'UE en janvier 2020 a permis au gouvernement britannique d'envisager un nouveau projet de loi ne nécessitant pas de se conformer aux exigences posées par le législateur européen. De ce point de vue, l'*Online Safety Act* témoigne de la capacité du Royaume-Uni à encadrer l'utilisation de nouvelles technologies et à établir ses propres standards en l'absence de règlementation supranationale. Toutefois, il convient de nuancer cette observation en rappelant que depuis 2021, le Royaume-Uni bénéficie d'une décision d'adéquation[42] au titre du RGPD, en ce qu'il assure un niveau de protection des données personnelles substantiellement équivalent à celui garanti par la législation de l'UE. Toutefois, à titre exceptionnel, cette décision est soumise à une clause de caducité et doit être renouvelée en juin 2025 ; toute divergence entre le droit européen et le droit britannique pourrait ainsi remettre en cause le niveau de protection adéquat. Par ailleurs, le RGPD n'est pas incompatible avec un contrôle de l'âge pour l'accès aux sites pornographiques ; il privilégie simplement un système de vérification respectueux de la vie privée par défaut et par conception.

Au-delà des contraintes technico-juridiques qu'elle pose, l'estimation de l'âge à l'aide d'algorithmes ne permet pas d'assurer avec certitude le filtrage des personnes mineures à l'entrée des sites pornographiques. À cette fin, il est nécessaire d'effectuer un véritable contrôle de l'âge de l'utilisateur, en ce qu'il constitue un attribut de son identité.

[40] British Standards Institution. (2018). Online age checking. Provision and use of online age check services. Code of Practice. https://shop.bsigroup.com/products/online-age-checking-provision-anduse-of-online-age-check-services-code-of-practice/standard/preview.

[41] Leloup, D. (2019). Comment un projet britannique de filtrage du porno a tourné à la catastrophe. *Le Monde.* https://www.lemonde.fr/pixels/article/2019/07/13/le-filtrage-du-porno-brxit-un-projet-britannique-qui-a-tourne-a-la-catastrophe-industrielle_5488904_4408996.html.

[42] Commission européenne. (2021). Décision d'adéquation constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D1773&from=EN.

### 2. *L'encadrement du contrôle de l'âge en tant qu'attribut de l'identité*

**Base légale du contrôle de l'âge.** Le RGPD interdit en principe tout traitement de données sensibles, sous réserve d'exceptions strictement énumérées[43]. Or, vérifier l'âge des utilisateurs de sites pornographiques revient à effectuer un traitement de données sensibles. En France, le contrôle de l'âge est licite, puisqu'il est indirectement requis par les articles 227-24 du Code pénal[44] et 23 de la loi du 30 juillet 2020[45]. Ce contrôle, en ce qu'il implique un traitement de données sensibles, répond à un objectif d'intérêt public (la protection des mineurs) et a été jugé proportionné à l'objectif poursuivi[46]. De plus, l'article 1er de la loi SREN impose aux sites pornographiques de garantir qu'aucun utilisateur n'accède à leurs contenus tant qu'il n'a pas prouvé sa majorité. La preuve de cette majorité doit être conforme aux exigences techniques présentées dans le projet référentiel de l'Arcom, publié en avril 2024 dans le cadre d'une consultation publique. Parmi les critères fixés dans le référentiel, celui de l'efficacité de la solution implique de *« distinguer de façon certaine les utilisateurs mineurs des utilisateurs majeurs »*[47]. L'Arcom précise que si la solution technique repose sur une estimation de l'âge de l'utilisateur, elle doit être paramétrée de sorte à exclure le risque qu'un utilisateur mineur soit considéré comme majeur (« faux positif »)[48] ; or, cette condition n'est pas encore satisfaite à l'état de l'art. Dès lors, la preuve de majorité ne peut reposer sur la seule estimation de l'âge ; le système de vérification doit intégrer un véritable contrôle de l'âge, sur la base d'un document témoignant de l'identité et/ou la date de naissance de l'utilisateur. Ce document constituerait le support de la vérification ; il peut s'agir d'une carte bancaire, d'une carte nationale d'identité, voire d'une « identité numérique » fournie par un service de l'État.

**Vérification de l'âge par le biais d'une carte de paiement.** La solution de vérification de l'âge par carte bancaire consiste à effectuer un « micropaiement » à l'aide du numéro de

[43] Article 9 du RGPD.
[44] L'article 227-24 du Code pénal prévoit notamment une peine de trois ans d'emprisonnement et 75 000 euros d'amende lorsque le contenu pornographique *« est susceptible d'être vu ou perçu par un mineur ».*
[45] L'article 23 de la loi du 30 juillet 2020 prévoit notamment que lorsqu'un éditeur de service en ligne permet à des mineurs d'accéder à du contenu pornographique en violation de la loi, le président du CSA (désormais l'Arcom) lui adresse une mise en demeure l'enjoignant de prendre des mesures pour empêcher cet accès.
[46] Cass. 1re civ., 5 janv. 2023, n° 22-40.017 : JurisData n° 2023-000021 ; Dalloz actualité, 19 janv. 2023, obs. J. Groffe-Charrier.
[47] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 12. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.
[48] Ibid.

carte bancaire de l'utilisateur[49]. Si l'accès au site est gratuit, le compte bancaire de l'utilisateur n'est pas débité ; l'idée de cette vérification ne repose donc pas sur le paiement en tant que tel, mais plutôt sur la validité de la carte bancaire[50]. Cette solution présente l'avantage de s'appuyer sur des infrastructures déjà existantes, ce qui faciliterait son intégration pour les plateformes hébergeant des contenus pornographiques ; en effet, les systèmes de paiement en ligne sont largement répandus et intègrent des mesures de sécurité robustes, ce qui en fait une solution privilégiée pour tout type de plateformes au regard de son efficacité opérationnelle. Toutefois, la vérification de l'âge par carte bancaire présente certaines limites ; d'abord, celle-ci est accessible aux mineurs possédant une carte de paiement, car en France, les mineurs peuvent être en possession d'une carte bancaire dès l'âge de 16 ans[51]. Cette solution serait davantage adaptée dans des pays tels que le Royaume-Uni, où il est nécessaire d'avoir 18 ans pour être titulaire d'une carte de crédit[52]. Dans tous les cas, un mineur peut avoir accès à des cartes prépayées ou utiliser celles de ses parents sans leur autorisation. Par ailleurs, cette preuve par micropaiement n'est pas accessible à tous les adultes, notamment ceux issus de milieux socio-économiques défavorisés ne possédant pas de carte bancaire, créant ainsi une différence d'accès basée sur des critères financiers. Enfin, certains utilisateurs pourraient être réticents à saisir leurs informations bancaires à l'entrée d'un site pornographique, au regard des risques de fraude et d'hameçonnage pouvant y être associés.

**Contrôle d'un document attestant de l'identité.** Le recours au contrôle d'un document attestant de l'identité de l'utilisateur doit être mis en balance avec l'impact potentiel sur sa vie privée, et ce, même si l'obligation de vérification d'âge impose aux plateformes un encadrement strict du traitement des données personnelles. Dans le cadre de l'accès aux sites pornographiques, la vérification de l'âge basée sur un document d'identité se décline en plusieurs variantes, selon que l'utilisateur fournit uniquement sa carte, ou qu'il fournit une preuve supplémentaire pour confirmer son identité[53]. La vérification « simple » par laquelle

[49] Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 7. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.

[50] CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

[51] Service public. Un mineur peut-il avoir un compte bancaire ou un produit d'épargne ? https://bit.ly/3VujK1R

[52] Renaissance numérique. (2022). *Contrôle de l'âge en ligne : pour une approche proportionnée et européenne*, page 27. https://www.renaissancenumerique.org/wp-content/uploads/2022/09/renaissancenumerique_controleage_rapport.pdf.

[53] Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 7. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.

l'utilisateur fournit uniquement sa carte d'identité nationale est peu contraignante dans sa mise en œuvre, mais présente des risques de fraude assez élevés ; le mineur souhaitant accéder au site peut utiliser la carte d'identité de ses parents, ou toute carte d'identité trouvée en ligne, en l'absence de stockage des cartes contrôlées. Ainsi, une méthode plus poussée consiste à comparer la photo sur la carte d'identité avec une photo ou vidéo prise par l'utilisateur[54] ; il s'agit d'un test de « détection du vivant », beaucoup plus fiable que la vérification de la seule carte d'identité, et utilisé notamment pour la vérification d'identité selon le référentiel PVID de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[55]. Toutefois, d'un point de vue technique, la vérification à partir d'une photo récente peut être complexe si la carte d'identité est ancienne. Par ailleurs, cette solution est particulièrement intrusive et pose le problème de son acceptabilité sociale. Enfin, le contrôle de l'identité de l'utilisateur peut également s'effectuer hors ligne, par le biais de « cartes à gratter » permettant de récupérer un identifiant et un mot de passe uniques, distribuées dans les grandes surfaces ou les bureaux de tabac par exemple[56]. Toutefois, cette solution apparaît comme étant stigmatisante pour les personnes souhaitant accéder à un site pornographique, remettant également en cause son acceptabilité sociale, et donc, son efficacité concrète.

**Utilisation de services numériques proposés par l'État.** L'utilisation de bases de données publiques ou d'un système d'authentification étatique pourrait permettre de vérifier l'âge des utilisateurs souhaitant accéder à certains sites. La vérification porterait sur un identifiant national (tel que le numéro de sécurité sociale ou l'identifiant France Connect) relié à un service numérique étatique. Toutefois, sans l'intervention d'un tiers permettant d'anonymiser la demande de vérification, l'État aurait connaissance du service depuis lequel la requête de vérification a été émise, et disposerait d'une liste de connexions de nature privée. Cela entraînerait un risque d'association entre l'identité de l'utilisateur et des informations intimes, corrélées à une supposée orientation sexuelle de l'individu[57]. Une solution proposée par le Pôle d'expertise de la régulation numérique (PEReN) consiste à recourir au « service de

[54] Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 7. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.
[55] CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.
[56] Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 7. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.
[57] Ibid.

garantie de l'identité numérique » (SGIN), consacré par un décret du 26 avril 2022[58]. L'utilisation de ce service implique néanmoins de disposer à la fois d'une carte d'identité électronique et d'un smartphone capable de lire la puce de la carte d'identité, en vue de fournir une attestation contenant uniquement les informations nécessaires à la vérification[59]. Ainsi, cette solution s'adresse à un public restreint et doit être envisagée en tant qu'alternative aux outils accessibles à tous. En outre, il apparaît pertinent de considérer l'utilisation de services étatiques comme un moyen d'exercice de la souveraineté des États, dans la mesure où celle-ci renvoie notamment à leur capacité à exercer un contrôle sur leurs infrastructures numériques, et à protéger les données de leurs citoyens contre les ingérences des services privés et/ou étrangers.

**Minimisation des données en raison de leur nature sensible.** Le principe de minimisation des données *« donne expression au principe de proportionnalité »*[60] car il impose que les données traitées soient *« pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités* [poursuivies] *»*[61]. Ainsi, quelle que soit la solution choisie, celle-ci doit impérativement minimiser la collecte de données, en vue d'assurer la protection de la vie privée des utilisateurs[62]. Dans la mesure où la vérification de l'âge peut impliquer d'effectuer une vérification de l'identité, celle-ci doit intégrer les principes de minimisation et de protection des données dès la conception et par défaut[63]. La garantie de cette protection est fondamentale au regard du traitement éventuel des données de navigation ; à partir des sites visités, il est possible de déduire l'orientation ou les préférences sexuelles d'un utilisateur. Or, une telle collecte d'informations aussi sensibles par les sites concernés est contraire aux dispositions du RGPD. Dès lors, la méthode de vérification choisie doit permettre de limiter la collecte de données personnelles au strict nécessaire, mais également de ne pas les conserver une fois la vérification effectuée, ni de les utiliser à d'autres fins, y compris commerciales. Pour garantir cette minimisation des données, la preuve de majorité doit être contenue dans un document dont les données identifiantes sont supprimées avant tout traitement. Pour cela, la CNIL recommande

[58] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».
[59] Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 8. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.
[60] CJUE, *Inspektor v Inspektorata kam Visshia sadeben savet,* 8 déc. 2022, aff. C-180/2,.point 96.
[61] Article 5.1, c. du RGPD.
[62] CNIL. (2021). Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.
[63] Articles 5 et 25 du RGPD.

l'intervention d'un « organisme tiers de confiance »[64] dans le processus de vérification, agissant en tant qu'intermédiaire pour protéger l'identité de l'utilisateur souhaitant accéder à un site pornographique.

Selon la CNIL, la vérification de l'âge par l'intermédiaire d'un tiers de confiance permettrait *« de garantir la protection de l'identité de l'individu et le principe de minimisation des données, tout en maintenant un haut niveau de garantie sur l'exactitude des données transmises »*[65]. Ce tiers serait chargé de transmettre la preuve d'âge, mais également la preuve que cette information émane d'un tiers de confiance agréé. La mise en œuvre technique de cette solution repose sur un mécanisme de « double anonymat »[66], car elle permet d'assurer la confidentialité de la vérification vis-à-vis du site à l'origine de la demande, ainsi qu'à l'égard du tiers vérificateur.

### ***B. La transmission de la preuve de l'âge protégée par le dispositif de «double anonymat»***

La protection de la vie privée des utilisateurs de sites pornographiques réside principalement dans le mécanisme de transmission du résultat de la vérification à l'utilisateur. À cette fin, le Laboratoire d'innovation numérique de la CNIL (LINC), a développé un mécanisme intégrant un protocole « zero-knowledge proof » (1), dont l'efficacité dépend de l'intervention d'un tiers vérificateur chargé de protéger l'anonymat des utilisateurs (2).

#### *1. La garantie de fiabilité du protocole zero-knowledge proof*

**Anonymisation des données identifiantes.** Le considérant 26 de la directive du 24 octobre 1995 sur la protection des données personnelles dispose que *« les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable »*. Ainsi, les procédés d'anonymisation permettent le traitement de données personnelles sans que celles-ci ne puissent être reliées à la personne

[64] CNIL. (2021). Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.
[65] CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.
[66] Laboratoire d'Innovation Numérique de la CNIL. (2023). Vérification de l'âge : l'argument économique. https://linc.cnil.fr/suite-demonstrateur-verification-de-lage-largument-economique-0.

auxquelles elles appartiennent. Dans le cadre de l'accès aux sites pornographiques, l'anonymisation vise à empêcher la collecte de l'identité, l'âge, la date de naissance, ou toute autre information permettant d'identifier (directement ou indirectement) les utilisateurs[67]. À cet effet, le mécanisme de transmission de preuve de l'âge développé dans le cadre d'un partenariat entre le PEReN, la CNIL et Olivier Blazy, professeur à l'Ecole polytechnique et chercheur en cryptographie, mérite une attention particulière. Rendu public le 21 juin 2022, ce mécanisme répond en tous points à la recommandation faite par la CNIL, à savoir le recours à un *« mécanisme de double anonymat empêchant, d'une part, le tiers de confiance d'identifier le site ou l'application à l'origine d'une demande de vérification et, d'autre part, faisant obstacle à la transmission de données identifiantes relatives à l'utilisateur au site ou à l'application proposant des contenus pornographiques »*[68]. Il convient de préciser qu'au sens du RGPD, ce mécanisme repose sur la pseudonymisation et non sur l'anonymisation des données ; le terme d'« anonymat » doit donc s'interpréter au sens cryptographique[69].

**Fonctionnement du mécanisme de « double anonymat ».** Le mécanisme de « double anonymat » permet de protéger la transmission de la preuve de l'âge en empêchant, d'une part, que le tiers vérificateur identifie le site à l'origine de la demande de vérification, et d'autre part, que le site à l'origine de la demande de vérification identifie l'individu concerné[70]. Le fonctionnement de ce mécanisme a pour intérêt de préserver la confidentialité des données transmises, tout en garantissant la fiabilité de la vérification d'identité. Si ce mécanisme est qualifié de « double », il y a en réalité trois traitements de données : le premier est réalisé par l'émetteur de la preuve d'âge ; le deuxième renvoie à la transmission de la preuve d'âge ; le troisième consiste à valider l'authenticité de la preuve pour autoriser l'accès au site pornographique. Le mécanisme de double anonymat repose sur un protocole sécurisé utilisant les « preuves à divulgation nulle de connaissance » (« zero-knowledge proof »), permettant aux utilisateurs du protocole de *« prouver qu'une situation est avérée sans avoir à révéler d'autres*

[67] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 12. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.

[68] CNIL. (2021). Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

[69] Laboratoire d'Innovation Numérique de la CNIL. (2022). Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée. https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee.

[70] Ibid.

*informations »*[71]. Cette solution cryptographique est d'ailleurs reconnue à l'échelle européenne ; dans le cadre de sa stratégie visant à rendre Internet plus sûr pour les enfants, la Commission européenne envisage de modifier le règlement eIDAS en vue de générer des *« attestations électroniques d'attributs valides et légalement reconnues à travers l'Union »*[72]. Le Parlement européen a également proposé d'y intégrer une « preuve à divulgation nulle de connaissance »[73], à l'image de la solution de double anonymat proposée par le PEReN et la CNIL. Cela implique de mobiliser un second concept cryptographique appelé « signature de groupe »[74]. La signature de groupe permet à l'utilisateur de prouver son appartenance à un groupe spécifique (ici, les adultes) tout en préservant son anonymat. En effet, ce procédé permet aux membres du « groupe » de signer des « challenges » (support de la preuve) pour un utilisateur, sans que celui-ci n'ait à révéler son identité[75]. Si le challenge est valide, cela signifie que l'utilisateur fait effectivement partie du groupe des personnes majeures, et qu'il est autorisé à accéder aux sites pornographiques. De cette manière, les signatures numériques certifient l'âge de l'utilisateur, tandis que le zero-knowledge proof prouve la connaissance d'une information sans la révéler.

**Fonctionnement du protocole zero-knowledge proof.** Le protocole de « preuve à divulgation nulle de connaissance » n'est pas un concept nouveau ; il a été introduit dans les années 1980 par les chercheurs Silvio Micali, Shafi Goldwasser et Charles Rackoff dans un document portant sur la complexité des connaissances des systèmes de preuves interactives[76]. Il repose sur des techniques cryptographiques avancées telles que les engagements réversibles et les preuves interactives pour réduire au maximum les risques d'erreur[77]. Ce protocole implique deux parties : le « prouveur » qui détient une connaissance secrète, et le « vérificateur » qui souhaite s'assurer que le prouveur possède cette connaissance[78].

---

[71] CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

[72] Parlement européen et Conseil de l'UE, (2024). Proposition de règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401183.

[73] Art. 1, 3°, a, 5° quater, et 6 bis, du projet de résolution législative du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique (Doc. COM (2021)0281 – C9-0200/2021 – 2021/0136(COD)).

[74] Laboratoire d'Innovation Numérique de la CNIL. (2022). Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée. https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee.

[75] Ibid.

[76] Coin Academy. Zero-Knowledge Proof, le nouveau protocole qui respecte la vie privée. https://coinacademy.fr/academie/explications-zero-knowledge-proof/

[77] Ibid.

[78] Pierre, J. (2024). Qu'est-ce que la preuve de connaissance nulle Zero Knowledge Proof ? https://www.mailinblack.com/ressources/blog/quest-ce-que-la-preuve-de-connaissance-nulle-zero-knowledge-proof/

Concrètement, le protocole zero-knowledge proof intègre plusieurs éléments attestant de sa fiabilité et de sa sécurité par rapport aux protocoles cryptographiques standards ; d'abord, les interactions entre le prouveur et le vérificateur permettent à ce dernier de poser des défis aléatoires, de sorte que le prouveur ne puisse pas les anticiper[79]. Le vérificateur répète cette formule un grand nombre de fois, afin de la valider de manière probabiliste ; plus les preuves sont répétées, plus la certitude augmente. De son côté, le prouveur intègre de la « randomisation cachée »[80] ainsi que d'autres problèmes complexes dans ses preuves. En outre, le protocole zero-knowledge proof respecte trois propriétés fondamentales ; la consistance, c'est-à-dire la véracité de l'information transmise ; la robustesse, à savoir la fiabilité de la technique utilisée ; et le zero-knowledge, qui empêche la transmission d'information supplémentaire au vérificateur. Ces propriétés cryptographiques permettent de garantir l'intégrité, l'authenticité et la confidentialité de la preuve. Ainsi, l'utilisation du protocole zero-knowledge proof respecte les principes posés par le RGPD, dans la mesure où aucune donnée n'est stockée ni partagée, conformément aux principes de confidentialité et de minimisation des données personnelles. De plus, cela permet à l'utilisateur de conserver un contrôle total sur ses données, garantissant ainsi son consentement éclairé au regard de l'utilisation de ce protocole.

**Implémentation du mécanisme à l'entrée des sites pornographiques.** L'installation du mécanisme de double anonymat déployé par le PEReN nécessite uniquement Docker ; le code source est en libre accès, modifiable et réutilisable sous réserve de mentionner la CNIL[81]. La coopération de trois entités est nécessaire à l'échange de la preuve au regard de la vérification d'âge : le site pornographique à l'origine de la demande de vérification ; un tiers accrédité pour effectuer la vérification de l'âge ; et une autorité certificatrice pour accréditer ces tiers[82]. À chaque demande de vérification, le site pornographique générera un « challenge » unique que l'utilisateur chargera sur le site du tiers accrédité. Ce tiers ne signera le challenge que si l'utilisateur a l'âge requis, puis lui transmettra le challenge signé. Enfin, le site validera la signature si celle-ci provient effectivement d'un tiers accrédité[83]. Par ailleurs, les challenges n'auront qu'une validité limitée dans le temps ; si ce n'était pas le cas, cela

[79] Pierre, J. (2024). Qu'est-ce que la preuve de connaissance nulle Zero Knowledge Proof ? https://www.mailinblack.com/ressources/blog/quest-ce-que-la-preuve-de-connaissance-nulle-zero-knowledge-proof/
[80] Le vérificateur pose des questions aléatoires que le prouveur ne peut pas anticiper afin de garantir la sécurité du protocole. Source : https://coinacademy.fr/academie/explications-zero-knowledge-proof/
[81] Laboratoire d'Innovation Numérique de la CNIL. (2022). Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée. https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee.
[82] Ibid.
[83] Annexe 2.

impliquerait de les garder en mémoire, ce qui ne serait pas conforme au RGPD. Dans son projet de référentiel publié en avril 2024, l'Arcom préconise une durée de validité d'une heure pour le challenge correspondant à la preuve d'âge, et pour consulter des contenus pornographiques sans nouvelle vérification[84]. Ainsi, l'une des principales difficultés susceptibles de remettre en cause l'efficacité de ce mécanisme concerne les éventuels échanges (gratuits ou non) de challenges, une fois qu'ils ont été signés par le tiers. D'après Olivier Blazy, il existe effectivement un risque de commercialisation des challenges, mais la contrainte d'un paiement (même minime) permettrait de décourager d'éventuelles pratiques destinées au contournement du mécanisme[85]. Le prix de la vérification varie selon le type de méthode envisagée ; par exemple, si une plateforme souhaite utiliser un dispositif d'analyse faciale, elle paiera un forfait correspondant à 50 centimes, voire 1 euro, pour chaque vérification[86]. Toutefois, afin d'éviter un accès discriminatoire aux sites pornographiques sur la base de critères financiers, le coût de la vérification doit être supporté par les sites pornographiques, sans être répercuté sur les utilisateurs. La solution proposée par la CNIL est celle de mettre en place un mécanisme régulier de paiement, par le biais d'un contrôle effectué par un service institutionnel, permettant de fixer le montant de la facturation en listant le nombre de challenges générés ; cela permettrait également d'éviter les risques de liens ou de recoupement entre l'utilisateur et le tiers, ainsi qu'entre le tiers et le site[87]. De cette façon, l'anonymat des utilisateurs serait strictement préservé.

Au-delà de sa fiabilité technique, l'efficacité du protocole zero-knowledge proof repose sur un acteur clé : le tiers vérificateur. Celui-ci doit garantir la confidentialité de la preuve de l'âge, ce qui suppose son entière indépendance à l'égard des éditeurs de sites pornographiques. Pour assurer cette indépendance, il est crucial que le tiers vérificateur soit soumis à des réglementations strictes et à des audits réguliers, garantissant ainsi qu'aucun conflit d'intérêt ne puisse compromettre la confidentialité et l'intégrité du processus de vérification.

[84] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 13. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.
[85] Annexe 1.
[86] Ibid.
[87] Ibid.

2. *La garantie de confidentialité du tiers vérificateur*

**Accréditation du tiers par une autorité certificatrice.** Le tiers vérificateur ne peut exercer son rôle d'intermédiaire sans y être autorisé ; il doit être accrédité par une autorité certificatrice, chargée d'organiser le système de vérification d'âge. Dès lors, il serait pertinent de désigner une autorité administrative indépendante pour fixer des standards de vérification applicables à tous les acteurs de l'écosystème. L'autorité certificatrice doit disposer de moyens techniques et légaux lui permettant d'établir un cadre normatif contraignant pour les tiers vérificateurs, d'instruire les demandes d'accréditation des tiers, et de procéder à des audits réguliers de leurs pratiques[88]. À ce titre, la loi SREN prévoit que les éditeurs et fournisseurs de services *« conduisent un audit des systèmes de vérification de l'âge qu'ils mettent en œuvre afin d'attester de la conformité de ces systèmes avec les exigences techniques définies par le référentiel »*[89]. Cet audit pourrait être exigé par l'Arcom, dans la mesure où cette autorité est chargée d'établir le référentiel technique auquel doivent se conformer les acteurs du contrôle d'âge (c'est-à-dire, les éditeurs de sites pornographiques, mais également les tiers vérificateurs). En cas de manquement, l'Arcom pourrait alors prononcer des sanctions graduées (avertissements, amendes, voire retrait d'accréditation). En outre, il serait pertinent d'envisager la création d'une autorité indépendante spécialement dédiée à la gouvernance du système de vérification d'âge, dont les prérogatives renforceraient la crédibilité et l'efficacité du dispositif de contrôle. Dans tous les cas, l'autorité certificatrice doit mettre en œuvre les dispositions contenues dans la loi SREN, et permettre à l'État français d'encadrer efficacement la vérification de l'âge des utilisateurs de sites pornographiques, ce qui témoignerait de sa capacité à exercer sa souveraineté numérique.

**Vérification de l'âge par le biais d'un service privé.** Si l'autorité certificatrice doit impérativement bénéficier d'une légitimité institutionnelle, le rôle de tiers vérificateur, en revanche, peut tout à fait être endossé par des services privés, tels que des banques, des fournisseurs d'accès internet[90], ou encore des fournisseurs d'identité (« identity providers ») privés. Les identity providers sont des organismes, publics ou privés, qui gèrent les identités

[88] CNIL. (2022). Rapport annuel, page 35. https://www.cnil.fr/sites/cnil/files/2023-05/cnil_-_43e_rapport_annuel_-_2022.pdf

[89] Article 1er de la loi SREN

[90] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 19. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.

numériques de leurs utilisateurs[91], et qui, à ce titre, détiennent une grande quantité d'informations, telles que leur âge. Ainsi, dans le cadre de la vérification de l'âge pour accéder aux sites pornographiques, il est possible d'envisager l'intervention de services tiers comme Google, Amazon ou encore Facebook, qui seraient techniquement capables d'intégrer le mécanisme de zero-knowledge proof. Dans leur fonction minimale, les identity providers gèrent les données d'identification et d'authentification de leurs utilisateurs ; ils peuvent également créer une identité numérique *ex nihilo*, c'est-à-dire créer une identité numérique à partir de données déclaratives[92]. Cela remet en cause la fiabilité de la vérification de l'âge de l'utilisateur, notamment pour Facebook qui ne contrôle pas l'âge des internautes au moment de leur inscription. Google, en revanche, se réserve la possibilité d'exiger une photocopie de leur pièce d'identité ou de leur carte bancaire, car certaines fonctionnalités ne sont accessibles qu'aux majeurs (par exemple, les vidéos YouTube non accessibles aux enfants). De son côté, Apple permet à ses utilisateurs de gérer un identifiant Apple ; aux États-Unis, une expérimentation est en cours pour intégrer une carte d'identité ou un permis de conduire dans l'Apple Wallet[93]. Ce « portefeuille » numérique pourrait d'ailleurs être utilisé lors des contrôles de sécurité dans certains aéroports américains[94]. Ainsi, Apple ne s'appuie pas sur une identité déclarative, mais émise par une autorité nationale de délivrance d'identité. Toutefois, déléguer la vérification de l'âge à des prestataires américains irait à l'encontre de l'affirmation de la souveraineté numérique de la France. Pour l'heure, certaines entreprises se sont positionnées pour assumer le rôle de tiers vérificateurs ; c'est notamment le cas d'Orange et de Docapost[95]. Ces tiers doivent impérativement faire preuve d'une fiabilité technique suffisante, sans quoi cette vérification resterait une prérogative strictement étatique.

**Vérification de l'âge par le biais d'un service étatique.** Par le biais du protocole zero-knowledge proof, le rôle de tiers vérificateur peut tout à fait être endossé par un service public sans que celui-ci soit en mesure de relier l'identité de l'internaute à sa demande d'accès au site pornographique. L'« identité » renvoie en premier lieu à l'identification des individus par l'État, et constitue donc une prérogative régalienne ; dès lors, il est pertinent d'envisager

[91] Levallois-Barth, C., Laurent, M. (2024). *Les acteurs de l'écosystème technique relatif aux identités numériques – Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique. Chaire Valeurs et Politiques des Informations Personnelles*. Institut Mines-Telecom. https://cvpip.wp.imt.fr/files/2024/02/2024-01-C-LEVALLOIS-M-LAURENT-acteurs-identites-numeriques.pdf.
[92] Ibid.
[93] Ibid.
[94] Anonyme. (2021). Apple teams up with TSA to enable digital identification at security checkpoints. *Future Travel experience.* https://bit.ly/4aTXXF6.
[95] Annexe 1.

une vérification de l'âge par le biais d'un service d'identité numérique fourni par l'État (tel que France Connect, la Poste, ou encore le service de garantie de l'identité numérique) ou à partir d'un identifiant national (tel que le numéro de sécurité sociale par exemple). Par ailleurs, d'après Olivier Blazy, il est tout à fait envisageable qu'une autorité publique assume à la fois le rôle d'autorité certificatrice et celui de tiers vérificateur ; par exemple, France Connect, même s'il n'a pas été pensé dans ce but, pourrait être un service étatique adapté pour fournir à la fois l'accréditation des services tiers et la transmission de la preuve de l'âge des utilisateurs[96]. Ainsi, la neutralité du tiers ne repose pas sur sa nature publique ou privée, mais sur son indépendance vis-à-vis du site pornographique, et sa confidentialité vis-à-vis des éventuels autres tiers impliqués dans le processus de vérification[97]. Par ailleurs, l'intervention d'un tiers vérificateur « étatique » serait une garantie supplémentaire de fiabilité ; en effet, l'identité de l'utilisateur serait certifiée par l'État, et les possibilités de contournement seraient minimisées. Cela permettrait également à l'État de réduire sa dépendance vis-à-vis des identity providers américains qui disposent aujourd'hui d'un quasi-monopole sur la gestion des identités en ligne et des données personnelles des internautes. Enfin, disposer d'un mécanisme de vérification d'âge pour l'accès aux sites pornographiques permettrait de proposer d'autres services numériques aux citoyens, et de contrôler plus efficacement les services en ligne restreints (jeux d'argents, vente d'alcool notamment). De ce fait, l'enjeu d'une vérification de l'âge par un service étatique est stratégique au regard de l'affirmation de la souveraineté numérique de l'État régulateur. Toutefois, du point de vue de l'acceptabilité sociale, les internautes pourraient craindre une surveillance étatique, voire un fichage de leurs informations intimes. Il est donc impératif de garantir aux utilisateurs la protection de leurs données de navigation par le biais du mécanisme de double-anonymat.

**Confiance des utilisateurs envers le tiers vérificateur.** Pour les utilisateurs, la contrainte d'une vérification de l'âge peut susciter une certaine méfiance et favoriser le contournement de la solution ; en ce sens, l'acceptabilité sociale du tiers vérificateur est un prérequis fondamental. La mise en place d'un mécanisme de vérification d'âge respectueux de la vie privée nécessite donc l'intervention d'un tiers de confiance strictement indépendant des

[96] Annexe 1.

[97] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 19. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.

parties prenantes. La neutralité du tiers est double : d'une part, il assure la transmission de la preuve sans être en mesure de savoir s'il a déjà traité une preuve du même utilisateur[98] ; d'autre part, la raison pour laquelle l'utilisateur demande un challenge (*i.e.*, l'accès à un site pornographique) restera inconnue pour le tiers vérificateur. Cette garantie de neutralité du tiers est primordiale dans le cadre de sa mission, d'où l'expression de tiers « de confiance ». Pour favoriser la confiance des utilisateurs, l'Arcom recommande aux éditeurs de sites pornographiques de disposer d'au moins deux méthodes de vérification différentes par le biais du double anonymat[99], ce qui pourrait permettre aux internautes de choisir entre plusieurs tiers vérificateurs (idéalement, un service étatique et l'autre privé). Par ailleurs, l'objectif d'aboutir à une solution *« zéro fichage et zéro piratage »*[100] repose avant tout sur la sécurité du traitement des données du l'utilisateur ; en ce sens, le tiers est soumis à une obligation générale de mettre en œuvre des mesures techniques et organisationnelles aux fins d'assurer la conformité et la sécurité du traitement[101]. Tel que cela a été explicité par Olivier Blazy, le mécanisme de double anonymat fonctionne sur la base d'un pseudonymat renforcé, dans la mesure où la provenance de la demande de preuve d'âge ne pourra en aucun cas être connue du tiers vérificateur ; le risque de fuite de données relatives à la navigation des utilisateurs sur des sites pornographiques est alors improbable[102]. En revanche, il n'est pas rare que les services numériques étatiques, détenteurs de millions de données personnelles appartenant à leurs citoyens, soient les cibles de cyberattaques. Récemment, France Travail a été victime d'une cyberattaque de grande ampleur, exposant potentiellement les données de 43 millions de personnes, incluant les noms, prénoms, numéros de sécurité sociale, identifiants France Travail, adresses mail et postales, ainsi que les numéros de téléphone[103]. Ainsi, le manque de confiance des citoyens envers les services numériques étatiques n'est pas uniquement lié à la crainte d'une surveillance ; il interroge également la robustesse insuffisante des infrastructures numériques de l'État face aux violations de données. À ce titre, le renforcement de la sécurité des services numériques de l'État est un prérequis indispensable au renforcement de la souveraineté numérique.

---

[98] Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques, page 19. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.

[99] Ibid.

[100] Interview du Ministre chargé du numérique, Jean-Noël Barrot, France info, 29 mai 2023.

[101] Articles 5.2 et 24 du RGPD.

[102] Annexe 1.

[103] CNIL. (2024). France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger. https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-proteger.

Au-delà de l'acceptabilité sociale de la solution de vérification d'âge, subordonnée à la volonté des citoyens de se conformer à l'obligation de vérification, l'efficacité de la régulation repose principalement sur l'action des éditeurs et hébergeurs de sites pornographiques, chargés de mettre en œuvre le filtrage des mineurs à l'entrée de leurs plateformes. En l'absence de coopération des acteurs soumis à la régulation, la capacité d'un État à imposer le blocage ou le déréférencement des sites est révélatrice de sa capacité à affirmer sa souveraineté numérique.

## II. La maîtrise du blocage étatique de l'accès aux sites pornographiques

La régulation française des sites pornographiques se traduit notamment par des mesures de blocage et de déréférencement des sites qui ne se conforment pas à l'obligation de vérification d'âge. Néanmoins, l'application de ces mesures se confronte aux impératifs communautaires et aux possibilités de contournement du blocage par les internautes (A). Par ailleurs, la restriction de l'accès aux sites pornographiques s'illustre à travers les tentatives d'appropriation du cyberespace par les États en quête d'affirmation de leur souveraineté numérique ; mais dans les sociétés démocratiques, ce contrôle ne peut s'opérer au détriment de la liberté d'expression (B).

### *A. Les difficultés de restriction territoriale de l'accès aux sites pornographiques*

Malgré l'adoption de la loi SREN et le renforcement des prérogatives de l'Arcom, la légitimité juridique du blocage demeure incertaine à plusieurs égards (1). De plus, ce blocage peine à être exhaustif car il peut aisément être contourné (2).

#### *1. Les incertitudes juridiques relatives au déréférencement et au blocage des sites*

**Base légale du géoblocage.** Le blocage géographique, ou « géoblocage », est une pratique consistant à limiter l'accès à certains produits ou services en fonction de la localisation géographique de l'utilisateur[104]. Son fonctionnement repose sur l'identification de l'adresse IP de l'utilisateur, à laquelle est associé un emplacement géographique (dont la précision s'apprécie à l'échelle du pays, voire de la ville). Sur la base de cette localisation, et en fonction des lois en vigueur, l'utilisateur peut être redirigé vers une version locale, se voir opposer une page d'avertissement, ou se voir totalement refuser l'accès au site[105]. Cette technique peut entraîner un cloisonnement des marchés, ce qui a mené le législateur européen à adopter le règlement (UE) 2018/302 du 3 décembre 2018 interdisant la pratique « injustifiée » du géoblocage, y compris lorsqu'il s'agit de services gratuits fournis par voie électronique[106]. Cette

[104] Robin, A. (2024). Chronique de droit de l'internet. *La Semaine Juridique Entreprise et Affaires n° 04*.
[105] Commission européenne. Bâtir l'avenir numérique de l'Europe. https://digital-strategy.ec.europa.eu/fr/policies/geoblocking.
[106] Ibid.

interdiction vise à supprimer les entraves à l'accès transfrontalier aux biens et services au sein du marché unique, mais réserve certaines possibilités de restriction pour des motifs légitimes, tels que le respect des droits de propriété intellectuelle ou l'existence de réglementations nationales. En ce qui concerne la France, l'article 6-I-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) dispose que le président du tribunal judiciaire (statuant selon la procédure accélérée[107]), peut prescrire à *« toute personne susceptible d'y contribuer »,* toutes mesures visant à empêcher ou à mettre fin à un préjudice causé par le contenu d'un service de communication accessible en ligne. Parallèlement, depuis la loi du 30 juillet 2020, l'article 227-24 du Code pénal punit le fait de rendre accessible aux mineurs des contenus à caractère pornographique[108]. Or, la quasi-totalité des sites pornographiques mettent à disposition de tous des contenus gratuits, enfreignant ainsi la loi vis-à-vis du contrôle de l'âge. Dès lors, le juge judiciaire peut ordonner le retrait et/ou le blocage des sites concernés à l'encontre de l'éditeur, de l'hébergeur, voire du fournisseur d'accès aux sites concernés par la régulation ; cela a été confirmé par la Cour de cassation dans sa décision du 18 octobre 2023, qui a rappelé que l'article 6-I-8 de la LCEN *« ne crée pas de hiérarchie entre l'action en justice menée contre l'hébergeur de sites pornographiques et l'action en justice menée contre le fournisseur d'accès Internet »*[109]. Ainsi, il est possible de solliciter la justice pour ordonner aux fournisseurs d'accès internet de bloquer l'accès à un site pornographique accessible aux mineurs, sans avoir préalablement engagé une action contre l'hébergeur ou l'éditeur des contenus. Toutefois, depuis l'entrée en vigueur de la loi de 2020, aucune demande de blocage n'est parvenue à son terme[110], ce qui a remis en question l'efficacité de cette procédure, et a incité le législateur français à renforcer son arsenal législatif.

**Apports de la loi SREN.** L'adoption de la loi SREN confère à l'Arcom un pouvoir de blocage « administratif » se concrétisant par le blocage « technique » par les fournisseurs d'accès Internet, sans avoir à obtenir l'aval du juge judiciaire. Cette nouvelle prérogative accordée à l'Arcom fait suite à de nombreuses mises en demeure adressées à des sites

[107] Procédure modifiée par la loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.
[108] *« Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique, y compris des images pornographiques impliquant un ou plusieurs animaux, ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur. »*
[109] Cass. Civ. 1ère, 18 oct. 2023, n° 22-18.926.
[110] Anonyme. (2023). Sites pornographiques : une demande de blocage renvoyée devant la cour d'appel. *Le Monde.*. https://www.lemonde.fr/pixels/article/2023/10/18/sites-pornographiques-une-demande-de-blocage-renvoyee-devant-la-cour-d-appel_6195243_4408996.html.

pornographiques, restées sans effet[111]. Depuis la saisine du tribunal judiciaire de Paris par l'Arcom en décembre 2021, la procédure de blocage à l'égard de cinq sites[112] était toujours en cours à la date de publication de son projet de référentiel technique (en avril 2024). Cette longue bataille juridique illustre la complexité du blocage des sites hébergeant des contenus pornographiques, tant par la longueur des procédures que par le nombre de contenus concernés ; un rapport du Sénat publié en 2022 a montré que 35% des vidéos sur Internet présentaient un caractère pornographique[113]. À la lumière de ce constat, l'apport principal de la loi SREN réside dans l'allègement de la procédure de blocage ; en cas de non-respect du référentiel établi par l'Arcom, celle-ci peut désormais bloquer et déréférencer tout site pornographique sans décision judiciaire préalable[114]. Toutefois, les conditions de ce blocage suivent une procédure stricte : l'Arcom doit d'abord adresser ses observations à l'exploitant du site concerné, qui dispose de 15 jours pour répondre ; puis une mise en demeure lui est adressée, permettant à l'exploitant de disposer de 15 jours supplémentaires pour adopter des mesures de restriction de l'accès des mineurs à ses contenus. Par ailleurs, la nécessité des mesures doit être réévaluée au moins une fois par an, et celles-ci doivent être levées si elles ne sont plus justifiées. Au regard de ces dispositions, deux groupes de soixante députés ont saisi le Conseil constitutionnel après l'adoption de la loi, contestant la durée excessive de ces mesures de blocage, ainsi que la brièveté du délai pour effectuer un recours en annulation[115]. Dans sa décision du 17 mai 2024, le Conseil constitutionnel a estimé que la durée maximale des mesures de blocage et de déréférencement était proportionnée au regard de l'objectif poursuivi par le législateur, à savoir, la lutte contre l'accès des mineurs à des contenus à caractère pornographique en ligne. Le Conseil constitutionnel a ainsi jugé l'article 2 de la loi SREN conforme à la Constitution, car le législateur, à travers cette disposition, *« a entendu mettre en œuvre l'exigence constitutionnelle de protection de l'intérêt supérieur de l'enfant et poursuivi l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public »*[116]. En ce sens, l'adoption de la loi SREN par le gouvernement français constitue un mode d'exercice de sa souveraineté numérique dans le

[111] Lucas, E. (2022). Blocage des sites pornographiques : la lutte de David contre Goliath. *La Croix*. https://www.la-croix.com/France/Blocage-sites-pornographiques-lutte-David-contre-Goliath-2022-10-04-1201236064.
[112] En décembre 2021, l'Arcom a mis en demeure cinq sites : Pornhub, Xnxx, Tukif, Xvideos et Xhamster, mais a été contrainte de saisir le tribunal judiciaire en mars 2022, en raison de leur inaction à changer leurs modalités de blocage.
[113] Sénat. (2022). Porno : l'enfer du décor. Rapport d'information n° 900 (2021-2022), tome I. https://www.senat.fr/rap/r21-900-1/r21-900-12.html.
[114] Article 2 de la loi SREN.
[115] Conseil constitutionnel, Décision n° 2024-866 DC du 17 mai 2024.
[116] Communiqué de presse du Conseil constitutionnel. Décision n° 2024-866 DC du 17 mai 2024. https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2024-866-dc-du-17-mai-2024-communique-de-presse.

cadre de la lutte contre le libre accès aux sites pornographiques. Or, si le blocage est conforme à la Constitution française, il ne l'est pas forcément au regard du droit de l'UE.

**Portée du principe du pays d'origine issu de la directive commerce électronique.** Le 6 mars 2024, le Conseil d'État a saisi la Cour de justice de l'Union européenne (CJUE) afin qu'elle examine la conformité du décret du 7 octobre 2021 au droit communautaire[117]. Cette saisine fait suite à une requête déposée par deux éditeurs de sites pornographiques basés en République Tchèque[118], qui ont invoqué une violation de la directive 2000/21/CE du 8 juin 2000 dite « directive commerce électronique ». En effet, conformément aux dispositions de cette directive, un État membre ne peut pas imposer à un fournisseur de plateforme établi dans un autre État membre des obligations trop imprécises : il s'agit du principe du pays d'origine. Selon ce principe, un fournisseur de service peut opérer dans toute l'Union européenne s'il respecte les conditions d'exercice de son activité dans l'État où il est établi[119]. En ce sens, la CJUE a récemment jugé que *« dans la lutte contre les contenus illicites sur Internet, un État membre ne peut pas soumettre un fournisseur d'une plate-forme de communication établi dans un autre État membre à des obligations générales et abstraites »*[120]. Or, de nombreux sites pornographiques, même s'ils sont implantés en dehors du territoire français, sont accessibles aux personnes résidant en France. Le principe du pays d'origine trouve-t-il à s'appliquer dans le cadre du décret relatif au blocage de ces sites ? Telle est la question posée par le Conseil d'État à la CJUE ; dans l'attente d'une réponse, le décret reste applicable. Toutefois, le Conseil d'État a d'ores et déjà écarté certains griefs des parties demanderesses, déclarant que le décret ne viole ni le principe de proportionnalité, ni la sécurité juridique, ni la liberté d'expression, ni le droit à un procès équitable[121]. En effet, qu'il existe ou non une règle de droit européen permettant l'application de dispositions visant à la protection des mineurs, les contenus pornographiques font partie d'une catégorie particulière de services, dont la restriction devrait,

[117] Conseil d'Etat. (2024). Accès en ligne aux contenus pornographiques : le Conseil d'État saisit la Cour de justice de l'Union européenne de l'enjeu de la protection des mineurs. https://www.conseil-etat.fr/actualites/acces-en-ligne-aux-contenus-pornographiques-le-conseil-d-etat-saisit-la-cour-de-justice-de-l-union-europeenne-de-l-enjeu-de-la-protection-des-min.

[118] Il s'agit précisément des sociétés Webgroup Czech Republic et NKL Associates sro, éditrices des sites Xvideos et XNXX.

[119] Dross, N. (2020). Fiche 7. La libre circulation des services ». Fiches de Politiques économiques européennes. Rappels de cours et exercices corrigés, sous la direction de DROSS Nicolas. *Ellipses,* p. 49-57. https://www.cairn.info/fiches-de-politiques-economiques-europeennes--9782340038387-page-49.htm.

[120] Piquard, A. & Reynaud, F. (2023). Numérique : les projets de loi français accusés d'empiéter sur le droit européen. *Le Monde*. https://www.lemonde.fr/pixels/article/2023/11/09/numerique-les-projets-de-loi-francais-accuses-d-empieter-sur-le-droit-europeen_6199179_4408996.html.

[121] Conseil d'Etat. (2024). Accès en ligne aux contenus pornographiques : le Conseil d'État saisit la Cour de justice de l'Union européenne de l'enjeu de la protection des mineurs. https://www.conseil-etat.fr/actualites/acces-en-ligne-aux-contenus-pornographiques-le-conseil-d-etat-saisit-la-cour-de-justice-de-l-union-europeenne-de-l-enjeu-de-la-protection-des-min.

à ce titre, faire l'objet d'une analyse spécifique par le juge européen. En outre, cette saisine de la CJUE met en lumière les tensions entre législation nationale et principes communautaires, tel que cela a été explicité par le Conseil d'État : *« Ce qui est en jeu est la possibilité pour la France d'imposer le respect d'au moins certaines de ses législations à des services numériques établis dans d'autres États membres de l'Union européenne »*. Ainsi, la capacité de l'État français à imposer ses lois à des sites pornographiques établis en dehors de son territoire, mais accessibles à ses citoyens, est révélatrice de sa capacité à exercer sa souveraineté numérique.

**Effets du DSA sur le blocage des très grandes plateformes.** La directive commerce électronique n'est pas la seule à remettre en cause la loi SREN : le 17 janvier 2024, la Commission européenne a rendu un avis circonstancié[122] sur certains amendements adoptés en séance, notamment sur les dispositions relatives aux sites pornographiques, considérant que celles-ci relèvent davantage du juge européen dans le cadre du *Digital Services Act* (DSA), que du juge national dans la cadre de la loi SREN[123]. En effet, dans son considérant 76, le DSA distingue les plateformes regroupant plus de 10% de la population européenne en les désignant comme des « très grandes plateformes », telles que Facebook ou YouTube, mais également des plateformes hébergeant des contenus pornographiques comme Pornhub, Stripchat et Xvidéos. Or, conformément au DSA, il appartient à la Commission européenne de réguler ces plateformes ; celles-ci doivent d'ailleurs se conformer à de nouvelles obligations, telles que la publication de rapports de transparence et d'évaluation de risques[124]. Elles devront également prendre des *« mesures d'atténuation afin de protéger les droits de l'enfant et empêcher les mineurs d'avoir accès à des contenus pornographiques en ligne, notamment grâce à des outils de vérification de l'âge »*[125]. Le terme « notamment » réfute le caractère obligatoire d'une vérification conforme aux dispositions de la loi SREN. Dès lors, l'ambition française de régulation des sites pornographiques semble s'approprier les prérogatives de la Commission européenne. Toutefois, il convient de s'interroger sur le champ de compétence concerné par la régulation ; s'agit-il d'une prérogative propre à l'UE, partagée, ou exclusive aux États membres ? Bien que la protection des mineurs face au libre accès aux sites pornographiques constitue un enjeu de santé publique, les modalités techniques de régulation de l'accès à ces contenus

[122] En vertu de l'article 6 de la directive du 9 septembre 2015, les avis circonstanciés donnent à la Commission le pouvoir de bloquer temporairement une loi nationale qu'elle estime contraire à la législation de l'UE.
[123] Le Priol, M. (2024). Numérique : la France accusée d'empiéter sur le droit européen. *La Croix*. https://www.la-croix.com/france/numerique-la-france-accusee-d-empieter-sur-le-droit-europeen-20240125.
[124] Commission européenne. (2023). La Commission désigne une deuxième série de très grandes plateformes en ligne au titre du règlement sur les services numériques. https://ec.europa.eu/commission/presscorner/detail/fr/IP_23_6763.
[125] Ibid.

constituent un domaine de compétence partagée avec l'UE, qui fixe un cadre général respecté par les États. Un compromis semble avoir été trouvé : afin de se conformer au droit européen, le pouvoir de régulation de l'Arcom ne s'exercera que sur les plateformes situées en France ou en dehors de l'Union européenne[126]. Cette portée limitée de la loi SREN remet en cause l'efficacité d'une régulation au seul échelon national, car les plateformes les plus visitées en France sont implantées dans d'autres États membres ; on compte notamment Pornhub et Xhamster à Chypre, ou encore Xvideos et Xnxx en République tchèque. Ces quatre plateformes totalisaient à elles seules 35,63 millions de visiteurs en France en janvier 2023[127]. Si les sites les plus visités par les Français sont hébergés dans d'autres pays de l'UE, cela rend-il la loi SREN obsolète ? À tout le moins, l'influence d'un ordre juridique supranational restreint considérablement la marge de manœuvre des États dans le cadre de la régulation de l'accès aux sites pornographiques.

Au-delà des difficultés légales du blocage, l'instauration de « barrières numériques » peut inciter au recours à des mécanismes de contournement par les internautes, ce qui rendrait caduque l'ensemble de la régulation sur l'accès aux sites pornographiques.

### 2. *L'accessibilité aux outils de contournement du géoblocage*

**Sites miroirs.** La première difficulté technique relative au blocage de l'accès aux sites pornographiques est d'abord liée à son efficacité dans le temps. En effet, il est fréquent qu'un site ayant fait l'objet d'une mesure de blocage soit reproduit de façon identique et référencé sous un autre nom de domaine : on parle alors de « site miroir ». Celui-ci est défini par l'article 6-2 de la LCEN comme *: « tout service de communication au public en ligne* […] *reprenant le contenu du service* […]*, en totalité ou de manière substantielle »*. Ainsi, pour créer un site miroir, il suffit de choisir un nom de domaine distinct de celui du site initial (par exemple modifier « .fr » en « .com »). Dans leur fonction première, les sites miroirs permettent d'assurer la continuité d'un service en cas de dysfonctionnement, de lenteur ou d'indisponibilité du site

[126] Le Priol, M. (2024). Numérique : la France accusée d'empiéter sur le droit européen. *La Croix*. https://www.la-croix.com/france/numerique-la-france-accusee-d-empieter-sur-le-droit-europeen-20240125

[127] 6,3 millions pour Xnxx, 7,4 millions pour Xvideos, 7,6 millions pour Xhamster, et 14,33 millions pour Pornhub. Source : https://fr.statista.com/statistiques/1417960/frequentation-sites-pornographiques-france/

principal[128]. Toutefois, dans le cadre du blocage de sites hébergeant des contenus illicites, la création de sites miroirs a pour effet de maintenir l'accessibilité des contenus, et constitue un moyen de contournement très utilisé : d'après l'Arcom, près de 35% des internautes se tournent vers un site illicite gratuit lorsqu'ils sont confrontés à un blocage[129]. Dans le cadre de la régulation de l'accès aux sites pornographiques, les sites miroirs constituent donc un obstacle à la bonne exécution des mesures de blocage ordonnées par l'Arcom ou le juge judiciaire. Pour lutter contre leur prolifération, un décret du 12 juin 2023 a désigné la Direction Générale de la Police, et plus précisément l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) pour procéder au blocage et au déréférencement du site visé[130]. En application de l'article 6-3 de la LCEN, cette autorité administrative est chargée de prendre toute mesure propre à empêcher l'accès aux sites miroirs dont l'accès a été interdit par décision judiciaire. Toutefois, cette procédure concerne uniquement les infractions prévues à l'article 6-I-7 de la LCEN[131], dont les contenus pornographiques sont exclus, puisqu'ils ne sont pas illicites en tant que tels. Par ailleurs, une loi du 25 octobre 2021 prévoit une procédure permettant de demander à l'Arcom le blocage de sites miroirs « contrefaisants »[132], mais n'est pas non plus adaptée à la lutte contre les contenus pornographiques en libre accès : d'une part, parce qu'elle est propre aux infractions de droit d'auteur ou de droit voisin ; d'autre part, parce qu'elle nécessite au préalable la condamnation judiciaire du site. Dès lors, l'Arcom doit être dotée de prérogatives similaires à celles de l'OCLCTIC pour ordonner le blocage et le déréférencement des sites pornographiques « miroirs » ; ces prérogatives peuvent être déduites de la loi SREN, sans toutefois être explicitement mentionnées.

**Configuration des paramètres DNS.** Conformément aux dispositions du décret de 2021, il est exigé des opérateurs qu'ils procèdent à l'arrêt de la connexion de l'internaute *« par tout moyen approprié, notamment en utilisant le protocole de blocage par nom de domaine*

[128] Ghozlan, S. (2023). Blocage et déréférencement des "sites miroirs" – analyse du décret du 12 juin 2023. *Village de la Justice*. https://bit.ly/4c3Arqf.
[129] Arcom. (2023). Blocage des sites miroirs : une coopération prometteuse entre l'Arcom et les ayants droit de l'audiovisuel pour renforcer la lutte contre le piratage, page 2. https://bit.ly/3X9r4AY.
[130] Léon, A. (2023). Blocage et déréférencement des sites miroirs : l'autorité compétente désignée par décret. *Lexbase.* https://www.lexbase.fr/article-juridique/96835775-brevesblocageetdereferencementdessitesmiroirslautoritecompetentedesigneepardecret.
[131] De façon exhaustive : l'apologie, négation ou banalisation des crimes contre l'humanité ; la provocation et apologie à la commission d'actes de terrorisme ; l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation sexuelle, de leur identité de genre ou de leur handicap ; la pornographie enfantine ; l'incitation à la violence, notamment incitation aux violences sexuelles et sexistes et les atteintes à la dignité humaine.
[132] Arcom. (2023). Blocage des sites miroirs : une coopération prometteuse entre l'Arcom et les ayants droit de l'audiovisuel pour renforcer la lutte contre le piratage. https://bit.ly/3X9r4AY.

*(DNS) »*[133]. À ce titre, les fournisseurs d'accès Internet ont recours au blocage par « Domain name system » (DNS), c'est-à-dire au filtrage du nom de domaine. Pour contourner ce filtrage, les utilisateurs peuvent aisément modifier les paramètres de leur connexion Internet pour interroger un autre serveur DNS que celui défini par défaut. Toutefois, cette pratique n'implique pas le chiffrement des données ; elle interroge simplement des serveurs DNS qui ne sont pas concernés par le blocage[134]. Un protocole récent appelé « DNS over HTTPS » (DoH) a été développé en vue de protéger la vie privée des utilisateurs, et peut être configuré dans des navigateurs Web pour chiffrer la requête de l'utilisateur[135]. Par ailleurs, il est tout à fait légal de changer sa configuration DNS, dans la mesure où cette modification dans les paramétrages ne vise pas uniquement à contourner le géoblocage. Déjà en 2014, la facilité de contournement du blocage DNS était pointée du doigt par les députés N. Goulet et M. Navarro dans leur amendement sur le projet de loi relatif à la lutte contre le terrorisme[136] : *« La première méthode de contournement de ce blocage consiste à modifier le réglage DNS de sa connexion (accessible très simplement dans les paramètres de configuration de l'ordinateur) pour transiter par un serveur DNS non soumis à la censure (étranger notamment). Ainsi, lorsque la Turquie a bloqué Twitter, des internautes ont peint sur les murs l'adresse du DNS public et gratuit de Google, qui n'était pas soumis aux ordres de blocage, au contraire des FAI turques. La seconde méthode consiste à rentrer directement l'adresse IP du site que l'on désire consulter (et qui nous aura été transmise, par exemple, par SMS), plutôt que son URL. Le DNS n'est donc plus nécessaire pour faire la traduction. C'est la raison pour laquelle cet article est inutile et doit être supprimé »*[137]. Si cet amendement a finalement été rejeté, il décrit précisément les limites du blocage d'Internet par les États. Ainsi, la simple configuration des paramètres DNS, accessible à tous, révèle la porosité des frontières numériques et la fragilité du contrôle étatique sur les contenus en ligne.

**Utilisation d'un réseau privé virtuel (VPN).** L'une des méthodes les plus courantes pour contourner le géoblocage est l'utilisation d'un réseau privé virtuel (VPN). Les VPN sont des logiciels, gratuits ou payants, qui permettent d'accéder au Web par d'autres adresses IP

[133] Article 5 du décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.
[134] Marino, L. (2016). Responsabilité civile et pénale des fournisseurs d'accès et d'hébergement. *Juris-Classeur Communication*, fasc. n° 670, 1re éd. 2016.
[135] Legrand, D. (2020). DNS over HTTPS (DoH) : au-delà de Firefox, une « question de confiance ». https://next.ink/6139/108770-dns-over-https-au-dela-firefox-question-confiance/.
[136] Désormais adoptée, il s'agit de la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.
[137] Sénat. (2014). Amendement présenté par Mme Nathalie GOULET et M. NAVARRO dans le cadre du Projet de loi relatif à la lutte contre le terrorisme. https://www.senat.fr/amendements/2014-2015/10/Amdt_1.html.

définies par le VPN plutôt que celle par défaut, généralement définie par le fournisseur d'accès Internet[138]. Chaque appareil pouvant être connecté à Internet possède une adresse IP, qui constitue le numéro d'identification lui étant attaché. L'utilisation d'un VPN permet de modifier virtuellement cette adresse IP ; ainsi, le géoblocage pourra être aisément contourné par un internaute français, devenu « étranger » par le recours au VPN. Cet outil de contournement est accessible à tous, et particulièrement connu des plus jeunes ; de nombreux créateurs de contenus destinés au grand public en font la promotion dans le cadre de sponsorisations sur des plateformes telles que YouTube. D'ailleurs, les VPN sont davantage utilisés par les 18-24 ans que par les 50-64 ans[139], et permettent aux mineurs de bénéficier (gratuitement ou à bas prix) d'une méthode efficace pour contourner la régulation de l'accès aux sites pornographiques. Certains États ont pu constater un rapport direct entre le blocage des sites pornographiques et le recours massif aux VPN ; aux États-Unis par exemple, la demande de VPN a augmenté de 967% après le blocage des sites pour adultes dans l'Utah en mai 2023, en raison de l'entrée en vigueur d'une loi obligeant les fournisseurs de contenus pornographiques à prendre des mesures « raisonnables » de vérification d'âge[140]. De ce fait, il est possible de présumer la similarité des réactions à l'entrée en vigueur de la loi SREN en France, d'autant plus en raison de l'accès libre et non contrôlé aux VPN. La solution serait-elle de soumettre le téléchargement des VPN à une vérification d'âge, à l'instar de l'accès aux sites pornographiques ? L'interdiction de la vente ou de la mise à disposition gratuite des VPN ne paraît pas être une solution adaptée ; en effet, un serveur VPN est avant tout un serveur proxy, c'est-à-dire un intermédiaire faisant transiter les requêtes par un serveur tiers. La différence majeure entre ces deux outils réside dans le chiffrement de bout-en-bout du trafic avec un VPN, contrairement à un proxy qui ne fait que relayer les requêtes sans chiffrement[141]. Dès lors, une approche prohibitive risquerait d'entraîner l'émergence d'autres solutions de contournement basées sur le fonctionnement des proxys. En outre, d'après Olivier Blazy, cela pénaliserait considérablement les entreprises, dans la mesure où celles-ci utilisent des VPN pour accéder à leur propre réseau et sécuriser les échanges de données internes[142]. L'interdiction des VPN empêcherait les salariés de faire du

[138] Groffe-Charrier, J. (2023). Contenus pornographiques - Contrôle de l'âge du public de contenus pornographiques : l'ouverture de la boîte de Pandore ? *Communication Commerce électronique* n° 9, étude 18.
[139] Statista Research Department. (2023). Part des Français utilisant un VPN (Virtual Private Network) en France en 2019, selon la tranche d'âge. https://fr.statista.com/statistiques/967931/part-francais-utilisant-vpn-par-age/.
[140] Rey N. (2023). La demande de VPN augmente de 967 % après le blocage des sites pour adultes dans l'Utah. https://securite.developpez.com/actu/344510/La-demande-de-VPN-augmente-de-967-pourcent-apres-le-blocage-des-sites-pour-adultes-dans-l-Utah-constate-vpnMentor-une-societe-de-VPN/.
[141] Lamb, N. (2024). VPN ou Proxy : Lequel choisir pour votre sécurité en ligne ? https://www.cyberghostvpn.com/fr/privacyhub/vpn-vs-proxy/
[142] Annexe 1.

télétravail de façon sécurisée, et parallèlement, les voyageurs commerciaux venant de l'étranger ne pourraient plus travailler depuis le territoire français ; toutes ces contraintes entraîneraient des conséquences néfastes sur l'économie française[143]. Ainsi, l'utilisation de VPN, bien qu'indispensables aux entreprises, permet aux particuliers de contourner les lois et règlementations des États, empêchant le blocage efficace des sites pornographiques, ce qui fragilise nécessairement leur souveraineté numérique.

À l'état de l'art, tout blocage peut être contourné grâce à des mesures techniques ou organisationnelles simples, car la structure même du réseau empêche tout contrôle exhaustif par les États. Toutefois, cette structure peut être modifiée ; la solution serait-elle de créer un réseau Internet décentralisé, un « Internet national » ?

## *B. Les perspectives de nationalisation d'Internet*

La lutte contre le libre accès aux sites pornographiques se heurte à la difficulté d'ériger des frontières au sein du cyberespace. En ce sens, la création d'un Internet « souverain » suppose une fragmentation de cet espace aligné sur les frontières nationales : dès lors, il serait possible d'opérer un contrôle exhaustif de l'accès à Internet (1). Néanmoins, le recours au blocage étatique de certains sites, jugés illicites, n'est pas sans effet sur la liberté d'expression, et constitue un moyen de censure inadapté aux sociétés démocratiques (2).

### *1. Le déploiement d'un réseau étatique centralisé*

**Maîtrise étatique des couches d'Internet.** Pour un État, l'affirmation de sa souveraineté numérique passe par le contrôle de ses infrastructures et services numériques. Dans sa conception opérationnelle, l'infrastructure d'Internet se décompose en quatre couches[144], à savoir : la couche physique ; la couche internet ; la couche transport ; et la couche application. Toutefois, Olivier Kempf dans sa définition du cyberespace, identifie trois couches

[143] Annexe 1.
[144] Au regard du modèle TCP/IP, car il y en a sept au regard du modèle OSI, mais celles-ci ne sont pas pertinentes en l'espèce.

: physique, logique et sémantique[145]. Cette classification présente l'avantage d'appréhender les enjeux de contrôle de l'espace comprenant tout l'Internet. Ainsi, pour envisager la création d'un Internet « national » véritablement isolé, les États doivent maîtriser les flux de données transitant sur ces différentes couches ; c'est à l'aune de ce contrôle que pourra pleinement s'exercer la souveraineté numérique dans le cadre de l'accès aux sites pornographiques. La couche « physique » d'Internet recouvre l'ensemble des infrastructures matérielles qui permettent d'acheminer les données : câbles, fibres optiques, équipements réseaux, centres de données, etc[146]. L'enjeu pour les États est donc de centraliser ces différentes infrastructures sur leur territoire national. Cette stratégie a été adoptée très tôt par la Chine, et plus récemment par la Russie, qui en 2014 a contraint les sociétés proposant leurs produits ou services sur Internet à destination de la population Russe, à implanter leurs serveurs sur le territoire Russe[147]. Si cette approche « localiste » a pour effet d'augmenter le coût des infrastructures nationales, elle permet également aux États de maîtriser la couche « physique » d'Internet. La couche « logique », quant à elle, regroupe les protocoles techniques qui permettent l'acheminement et le routage des données. À ce niveau, les États peuvent imposer leurs propres protocoles « nationaux » en les rendant incompatibles avec les standards internationaux[148]. Enfin, la couche « sémantique » renvoie à l'ensemble des contenus, services et applications accessibles sur Internet ; il s'agit de la couche la plus complexe à appréhender et à représenter d'un point de vue géographique[149], ce qui explique les difficultés d'une restriction territoriale de l'accès aux sites pornographiques par les États. Ainsi, à travers la maîtrise de ces trois couches, les États cherchent à maîtriser le cyberespace, comme un territoire à conquérir, à contrôler, à surveiller. Pour envisager la création d'un Internet « national », il convient d'adopter une approche comparative basée sur des solutions étatiques déjà opérationnelles. Si les tentatives d'appropriation de l'Internet par les États sont nombreuses, les cas chinois et russe constituent des exemples particulièrement pertinents, *a fortiori* au regard de l'illégalité de l'accès aux sites pornographiques dans ces deux pays.

---

[145] Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions*, 30, 141-149. https://doi.org/10.3917/infle.030.0141.

[146] Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote,* 152-153, 3-21. https://doi.org/10.3917/her.152.0003.

[147] Delesse, C. (2016). Chapitre V. La gouvernance d'Internet. *NSA National Security Agency*. *L'histoire de la plus secrète des agences de renseignement*, sous la direction de DELESSE Claude. Paris, Tallandier, « Hors collection », p. 325-329. https://www.cairn.info/nsa-national-security-agency--97910210086 32-page-325.htm.

[148] Cattaruzza, A. & Buisson, J. (2023). *La Cyberdéfense. Politique de l'espace numérique.* Paris, Armand Colin, « Collection U », p. 57-65. https://www.cairn.info/la-cyberdefense--9782200634223-page-57.htm.

[149] Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote,* 152-153, 3-21. https://doi.org/10.3917/her.152.0003.

**Grand Pare-feu de la Chine et filtrage des requêtes.** Dès l'essor d'Internet, le gouvernement chinois a cherché à créer un Internet « national » : en juin 2000, le Président de l'Académie des Sciences de Shanghai, Jiang Mianheng, l'exprimait en ces termes : *« La Chine doit bâtir un réseau national indépendant de l'Internet global ».* Ainsi, l'Internet chinois s'est développé par le biais d'une régulation très aboutie, à l'aide d'outils spécifiques comme Baidu (moteur de recherche), Tencent QQ (messagerie instantanée) et Weibo (réseau social)[150]. Conçu à la fin des années 1990, ce « Bouclier doré »[151] vise à maintenir le contrôle du gouvernement sur les activités en ligne et les communications de sa population d'internautes. Il recouvre un ensemble de dispositions normatives et techniques, telles que la surveillance des « backbones » et le filtrage des données en temps réel[152]. Les backbones ou « dorsales Internet » constituent l'architecture du réseau Internet chinois, puisqu'ils forment les seuls points d'accès au pays[153] ; ces dorsales sont contrôlées par des entreprises d'État comme *China Telecom, China Unicom et China Mobile*, qui gèrent les principaux points d'échange Internet et les câbles sous-marins, assurant ainsi une maîtrise quasi totale des flux de données entrant et sortant du pays[154]. Leur nombre restreint facilite l'installation de filtres et de logiciels spécialisés pour contrôler l'accès aux sites Web, qu'ils soient locaux ou étrangers. À ce titre, le chercheur Louis Pétiniaud, docteur de l'Institut français de géopolitique et chercheur post-doctoral en géopolitique des infrastructures Internet et du routage des données numériques, a déclaré que *« pour fermer un réseau, il faut en général essayer de réduire son nombre de portails vers l'extérieur, pour pouvoir exercer un contrôle plus ferme dessus »*[155]. Le Grand Pare-feu chinois a été installé sur les backbones, permettant au gouvernement de contrôler l'accès général à Internet. Par ailleurs, la Chine possède un système de filtrage consistant à bloquer l'accès des internautes à des sites en fonction de leur adresse IP et de leur nom de domaine. En 2021, le Grand Pare-feu a déployé une nouvelle capacité de détection passive du trafic entièrement chiffré en temps réel, ce qui lui permet désormais de bloquer massivement les protocoles de contournement[156]. Cette méthode,

---

[150] Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote,* 152-153, 3-21. https://doi.org/10.3917/her.152.0003.

[151] Delesse, C. (2016). Chapitre V. La gouvernance d'Internet. *NSA National Security Agency*. *L'histoire de la plus secrète des agences de renseignement*, sous la direction de DELESSE Claude. Paris, Tallandier, « Hors collection », p. 325-329. https://www.cairn.info/nsa-national-security-agency--9791021008632-page-325.htm.

[152] Harrel, Y. (2021). Comparatif des cyberpuissances : Etats-Unis, Chine, Russie » ? *Revue Conflits*. https://www.revueconflits.com/comparatif-cyberpuissances/.

[153] Arifon, O. (2009). Les diverses facettes du contrôle d'Internet en Chine. *Hermès, La Revue*, 2009/3 (n° 55), p. 155-158. DOI : 10.4267/2042/31515 https://www.cairn.info/revue-hermes-la-revue-2009-3-page-155.htm.

[154] Ibid.

[155] Jerome, E. (2023). Le Turkménistan veut créer son propre réseau Internet coupé du monde. *Novastan.* https://bit.ly/4c7gnDq.

[156] Anonyme. (2023). How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. https://www.usenix.org/system/files/sec23fall-prepub-234-wu-mingshi.pdf..

basée sur des règles heuristiques, remet en cause l'idée que le blocage étatique de certains sites est infaillible, et que l'utilisation d'outils de contournement est indétectable. Au regard de l'accès aux sites pornographiques, le Grand Pare-feu renforce le cadre légal très strict qui incrimine déjà la pornographie en Chine, puisque la simple consultation de tels sites constitue une infraction pénale sévèrement réprimée. D'ailleurs, la Chine a maintes fois attaqué Google au titre de la diffusion d'images pornographiques accessibles via son moteur de recherche[157]. Le gouvernement exige également que les fournisseurs d'accès à Internet et les plateformes Web surveillent leurs internautes ; ils sont légalement responsables du contenu publié par les utilisateurs sur leurs services[158]. En outre, le blocage des sites pornographiques est facilité par la capacité de la Chine à contrôler les flux de données transitant par le biais de son Grand Pare-Feu. Le filtrage renforcé des requêtes d'accès à ces sites représente donc un moyen pour Pékin d'affirmer sa souveraineté numérique sur son territoire.

**Runet souverain et contrôle d'Internet.** La politique numérique des autorités russes témoigne d'une volonté croissante de régulation et de contrôle d'Internet. Depuis le retour de Vladimir Poutine à la présidence en 2012, Moscou a intensifié ses efforts pour imposer des listes de sites interdits et relocaliser les données des internautes russes sur le territoire national, tout en réprimant sévèrement les propos en ligne critiques envers le pouvoir : pas moins de 87 000 URL ont été interdites en 2016, en vertu de la loi « Lougovoï »[159]. La nouvelle loi sur le « Runet souverain » signée en mai 2019 marque un tournant majeur, passant d'une logique de contrôle des contenus à une logique de maîtrise des infrastructures numériques. Cette loi illustre le phénomène de fragmentation de l'Internet mondial, et constitue un point de non-retour pour la Russie vers la création d'un « Internet national » sous contrôle étatique. Or, contrairement à la Chine qui a construit son réseau Internet « by design » pour faciliter son contrôle dès les années 1990, à la même époque, la Russie se disloquait de l'URSS, ce qui a mené à un développement relativement anarchique de l'Internet russe[160]. En ce sens, la loi sur le Runet souverain illustre la volonté du gouvernement à renforcer son emprise sur le réseau national. En ce qu'il s'agit du blocage des sites pornographiques, la loi fédérale sur « L'information, les

[157] Elegant, S. (2009). Chinese Government Attacks Google Over Internet Porn. *Time.* https://time.com/archive/6947092/chinese-government-attacks-google-over-internet-porn/.
[158] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[159] Nocetti, J. (2019). La Russie en quête de son « Internet souverain ». *La revue des médias.* https://larevuedesmedias.ina.fr/la-russie-en-quete-de-son-internet-souverain.
[160] Derivry, T. (2022). [INTERVIEW] LA SOUVERAINETÉ NUMÉRIQUE RUSSE EN 5 QUESTIONS AVEC KEVIN LIMONIER. https://www.sciencespo.fr/public/chaire-numerique/2022/10/18/interview-la-souverainete-numerique-russe-en-5-questions-avec-kevin-limonier/.

technologies de l'information et la protection de l'information » de 2006 interdit la diffusion de contenus pornographiques et prévoit des sanctions pénales pour les contrevenants[161]. Or, les efforts déployés jusqu'à présent, comme le blocage de certains sites par le Roskomnadzor[162], se sont avérés insuffisants pour endiguer la diffusion de ces contenus. Désormais, l'objectif de Moscou rappelle l'approche chinoise, puisqu'il vise non seulement à contrôler les contenus, mais également à exercer une maîtrise sur l'ensemble des services numériques (moteurs de recherche, réseaux sociaux, plateformes vidéo, etc.) ainsi que sur l'infrastructure du cyberespace russe (protocoles techniques, routeurs, etc.). Toutefois, comme le rappelle Kevin Limonier, l'infrastructure russe *« a été conçue dans un esprit d'ouverture et de circulation maximale de l'information, sans aucune sécurité intégrée »*[163]. Cette approche est conforme à l'esprit originel de l'Internet, comme le souligne Louis Pouzin, l'un des pères fondateurs de l'Internet, qui estime que pour sécuriser véritablement Internet, il faudrait le reconstruire entièrement sur de nouvelles bases[164]. Ce constat met en lumière les difficultés d'une régulation exhaustive de l'accès aux sites pornographiques, en raison de la nature même d'Internet.

**Système d'exploitation souverain.** L'affirmation de la souveraineté numérique passe donc par la création d'un Internet « souverain » : si les flux de données sont maîtrisés au niveau national, il reste à intégrer des systèmes d'exploitation agréés par les autorités publiques. Tel que défini par la CNIL, le système d'exploitation est *« la brique logicielle la plus proche du matériel informatique, allouant les ressources disponibles (ressources de calcul, mémoire, accès aux périphériques) aux différents éléments applicatifs qui en font la requête »*[165]. Dans le cadre de la souveraineté numérique, et à l'image de la maxime « Code is law » il est pertinent d'établir un parallèle entre les systèmes d'exploitation et les règles normatives d'un État. En effet, dans le cyberespace, le système d'exploitation joue un rôle similaire à la Constitution dans l'organisation et le fonctionnement d'un État. Tout comme la Constitution détermine les règles de base d'un pays, le système d'exploitation est le logiciel de base qui gère les ressources d'un ordinateur et permet le fonctionnement des autres programmes. Cette théorie a été développée par Pierre Bellanger dans ses *Archives de philosophie du droit* publiées en 2015 : *« Ces systèmes*

[161] Richter, A. (2021). *La réglementation des médias sociaux en Russie*. IRIS Extra, Observatoire européen de l'audiovisuel. https://rm.coe.int/iris-extra-2021fr-reglementation-des-medias-sociaux-en-russie/1680a3f8c7.
[162] Derivry, T. (2022). [INTERVIEW] LA SOUVERAINETÉ NUMÉRIQUE RUSSE EN 5 QUESTIONS AVEC KEVIN LIMONIER. https://www.sciencespo.fr/public/chaire-numerique/2022/10/18/interview-la-souverainete-numerique-russe-en-5-questions-avec-kevin-limonier/.
[163] Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote*, 152-153, 3-21. https://doi.org/10.3917/her.152.0003.
[164] Madelaine, N. (2013). Louis Pouzin : "L'Internet doit être refait de fond en comble", *Les Échos, n*°21442, p. 23.
[165] CNIL, « Système d'exploitation (ou « operating system », OS) ». Disponible en ligne : https://www.cnil.fr/fr/definition/systeme-dexploitation-ou-operating-system-os.

*d'exploitation se mettent en réseau, échangent constamment. Ils deviennent notre interface avec Internet, notre intermédiation avec les autres et le monde. Ils sont l'intelligence d'accès au réseau et le contrôlent. À la manière des lois qui s'appuient sur la Constitution, toutes les applications et services dépendent de ce réseau de systèmes »*[166]. Ainsi, en maîtrisant le code source et les fonctionnalités du système d'exploitation, les autorités pourraient intégrer des mécanismes de filtrage et de blocage plus efficaces. L'une des approches possibles serait l'intégration de listes noires de sites pornographiques directement dans le système d'exploitation ; ces listes, gérées par les autorités, permettraient de bloquer automatiquement l'accès aux sites prohibés, sans nécessiter l'installation de logiciels tiers ou de configurations complexes. Les mécanismes de filtrage pourraient être basés sur des analyses de contenu, des empreintes numériques ou des listes d'adresses IP et de noms de domaine. Au-delà de la question spécifique de la pornographie, les aspirations grandissantes des États pour le contrôle d'Internet soulèvent des inquiétudes quant aux risques de profilage et de censure de la liberté d'expression.

En effet, les tentatives d'appropriation d'Internet par les États compromettent l'exercice des droits et libertés fondamentaux des individus : si les autorités maîtrisent l'ensemble des flux transitant sur le cyberespace, le risque majeur est qu'elles soient tentées de bloquer d'autres types de contenus jugés indésirables, tels que les contenus politiques ou les critiques à l'encontre du gouvernement.

2. *Les risques de censure de la liberté d'expression*

**Sites pornographiques et liberté d'expression.** La liberté d'expression est consacrée par plusieurs instruments juridiques internationaux, notamment par l'article 19 de la Déclaration universelle des droits de l'homme (DUDH) qui dispose que : *« Tout individu a droit à la liberté d'opinion et d'expression ; ce droit inclut la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, par n'importe quel moyen d'expression »*. De même, l'article 10 de la Convention européenne des droits de l'Homme (ConvEDH) protège la liberté d'expression, tout en permettant des restrictions *« nécessaires dans une société démocratique »* pour des motifs légitimes, tels que la protection

[166] Bellanger, P. (2015). Souveraineté numérique et ordre public. *Archives de philosophie du droit*, 2015/1 (Tome 58), p. 285-296. https://www.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285.htm.

de la sécurité nationale, la prévention du crime, la protection de la santé ou de la morale, etc. Ainsi, la liberté d'expression n'est pas absolue et peut faire l'objet de restrictions. Toutefois, l'article 10, paragraphe 2 de la ConvEDH prévoit que toute ingérence à la liberté d'expression doit être prévue par la loi. En ce sens, la libre circulation de l'information au sein d'Internet constitue une manifestation fondamentale de la liberté d'expression : dans toute démocratie, cette liberté recouvre à la fois le droit de communiquer, de diffuser des informations et des idées à d'autres personnes, mais également le droit de recevoir des informations et des idées en provenance d'autrui[167]. Dans le cas particulier des contenus pornographiques, d'aucun pourrait arguer que la pornographie est une forme de discours protégée par la liberté d'expression. Cet argument repose sur l'idée que la pornographie, bien que controversée, relève de la liberté individuelle et de l'autonomie personnelle. Toutefois, les restrictions à cette forme de liberté d'expression visent avant tout à protéger les mineurs ; il s'agit à la fois d'un enjeu de santé publique et d'ordre public. Dès lors, la diffusion de contenus pornographiques, même si elle constitue un moyen pour les individus d'exercer leur liberté d'expression, fait l'objet d'une restriction prévue par la loi.

**D'un blocage arbitraire...** Le blocage d'Internet est un phénomène répandu parmi les États membres du Conseil de l'Europe. Ses impacts sur la liberté d'expression ont été mis en lumière dès 2011, lorsque le Rapporteur spécial de l' Organisation des Nations unies (ONU) sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, a souligné dans son rapport annuel les différents moyens par lesquels les États censurent de plus en plus les informations en ligne, notamment via le recours au blocage arbitraire, et qu'à ce titre, *« toute restriction à la liberté d'expression doit satisfaire aux critères stricts du droit international des droits de l'homme »* [168]. Par ailleurs, si le Rapporteur considère que le blocage peut être justifié pour la pédopornographie, qui constitue une exception évidente, il ne dit rien sur le blocage de la pornographie en tant que telle. Le rapport précise simplement que pour tout blocage, le cadre juridique national doit être suffisamment précis et prévoir des garanties effectives contre les usages abusifs. Selon la jurisprudence de la CEDH, toute mesure de blocage d'Internet par les États doit respecter trois critères : avoir un fondement juridique clair ; poursuivre un but légitime énuméré à l'article 10.2 de la Convention ; et être proportionnée et

[167] Parlement européen. (1997). Rapport sur la communication de la Commission sur le contenu illégal et préjudiciable sur le réseau Internet (COM(96)0487 - C4-0592/96). https://www.europarl.europa.eu/doceo/document/A-4-1997-0098_FR.html.

[168] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

nécessaire à ce but légitime[169]. Les États doivent donc justifier ces restrictions d'accès, avec un contrôle judiciaire pour prévenir les abus. Enfin, les juridictions nationales doivent s'assurer que le blocage est ciblé et proportionné, n'affectant que le contenu spécifique visé. En France, les modalités de blocage des sites pornographiques accessibles aux mineurs sont prévues par la loi[170] ; ce blocage s'inscrit dans un objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public[171] ; et sa durée maximale n'est pas disproportionnée au regard de l'objectif poursuivi par le législateur[172]. Toutefois, cette censure administrative fait peser sur les fournisseurs d'accès une responsabilité équivalente à celle des hébergeurs[173], ce qui va à l'encontre des recommandations de l'ancien Rapporteur spécial, Frank Larue ; en effet, il préconise que la censure ne devrait jamais être déléguée à une entité privée, et que *« nul ne devrait être tenu responsable d'un contenu diffusé sur Internet s'il n'en est pas l'auteur »*[174]. Il précise qu'aucun État ne devrait obliger les intermédiaires à censurer en son nom. Dans certains pays, comme le Chili et le Brésil, des projets de loi visent justement à protéger les intermédiaires de cette responsabilité, puisqu'ils ne sont pas soumis à l'obligation de bloquer les contenus illites, sauf s'ils en sont notifiés par une ordonnance de la cour[175]. En France, le régime de responsabilité « limitée » des intermédiaires techniques comme les hébergeurs, prévu par la LCEN, s'accompagne en réalité de nombreuses obligations qui ont pour effet de leur transférer la régulation des contenus en ligne. Les hébergeurs, par crainte des condamnations judiciaires, peuvent être ainsi poussés à une censure préventive de certains sites, même lorsque leur illicéité n'est que « vraisemblable » et non « manifeste ». Cette insécurité juridique pourrait dès lors conduire à privatiser la régulation de l'expression en ligne au détriment des libertés. De ce fait, les prérogatives accordées à l'Arcom, même si elles ont pour but d'alléger la procédure de blocage, soulèvent des interrogations quant à la portée de la responsabilité des intermédiaires. En Grande-Bretagne, où la législation sur les contenus pornographiques est historiquement conservatrice, le gouvernement a confié le blocage des sites aux fournisseurs d'accès. Selon

[169] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[170] Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales ; Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.
[171] Communiqué de presse du Conseil constitutionnel. Décision n° 2024-866 DC du 17 mai 2024. https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2024-866-dc-du-17-mai-2024-communique-de-presse.
[172] Ibid.
[173] Cass. Civ. 1ère, 18 oct. 2023, n° 22-18.926.
[174] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[175] Ibid.

l'ONG Open Rights Group, les listes de sites bloqués par ces fournisseurs ne se sont pas limitées à la pornographie ; des sites liés au partage de fichiers et certains réseaux sociaux y figurent également[176]. Au total, sur l'année 2014, 20% des sites les plus visités auraient été bloqués par ces filtres, alors même que les sites pornographiques ne représentaient que 4% des sites les plus visités, d'après Jim Killock, le directeur de l'ONG[177]. En effet, les systèmes de blocage ne sont pas infaillibles : ils engendrent inévitablement des erreurs avec des faux positifs (sites bloqués à tort) et des faux négatifs (sites illicites non bloqués). En Australie également, le gouvernement a mis en place à la fin des années 2000 un système de filtrage de sites Web dans le cadre de la lutte contre la pédopornographie en ligne. Cependant, après la fuite de la liste des sites bloqués, il a été constaté que celle-ci comportait non seulement des sites bloqués par erreur, mais aussi des sites interdits pour d'autres raisons ; sur cette liste, figuraient notamment plusieurs sites de poker en ligne, des sites liés au satanisme, ou encore des sites consacrés aux troubles alimentaires[178]. Dès lors, au regard des risques de censure injustifiée, des mesures de blocage ne doivent être prises que si le filtrage cible un contenu spécifique et clairement identifié comme étant illégal, sur la base d'une décision rendue par une autorité compétente, et susceptible d'être réexaminée par un tribunal ou un organe de régulation indépendant et impartial, conformément à l'article 6 de la Convention européenne des droits de l'homme. Ce n'est qu'à travers la mise en place de garanties suffisantes de protection de la liberté d'expression que les sociétés démocratiques pourront lutter contre l'accès illégal des mineurs aux sites pornographiques.

**…À un blocage autoritaire.** Les États autoritaires sont particulièrement enclins à recourir à la censure en ligne par le biais du blocage de sites Web (y compris les sites pornographiques) dans le but de contrôler les flux d'informations, ce qui a pour effet de restreindre les libertés individuelles. En Arabie saoudite, où la censure politique est particulièrement constatée, s'ajoute à l'interdiction de la pornographie celle des contenus jugés « immoraux » : les images présentant des décolletés ou des nudités partielles sont interdites, tout comme les contenus faisant référence à l'homosexualité[179]. De très nombreux sites Web se retrouvent donc bloqués. Afin de maintenir à jour sa liste noire des sites interdits, le ministère de l'Intérieur saoudien incite d'ailleurs les internautes à dénoncer les sites considérés comme

[176] Assemblée parlementaire du Conseil de l'Europe. (2022). Pour une évaluation des moyens et des dispositifs de lutte contre l'exposition des enfants aux contenus pornographiques », Rapport | Doc. 15494. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=29890&lang=fr.
[177] Ibid.
[178] Leloup, D., Untersinger, M., & Reynaud, F. (2015). L'impossible censure des sites pornographiques. *Le Monde.* https://www.lemonde.fr/pixels/article/2015/08/04/une-breve-histoire-de-la-censure-des-sites-pornographiques_4711451_4408996.html.
[179] Ibid.

« immoraux » pour les ajouter à cette liste de blocage[180]. Par ailleurs, dans son rapport sur la liberté d'expression, Frank Larue exprime sa préoccupation quant à la tendance émergente du blocage temporaire ou « opportun » d'Internet, visant à empêcher les utilisateurs de diffuser des informations lors de moments politiques clés, tels que les élections, les périodes d'agitation sociale ou les commémorations politiques et historiques[181]. En effet, ce phénomène a été observé lors des manifestations dans les régions du Moyen-Orient et d'Afrique du Nord au moment du Printemps arabe ; les sites Web des partis d'opposition, des médias indépendants et des plateformes de réseaux sociaux comme X (ex-Twitter) et Facebook ont été bloqués[182]. De cette manière, les gouvernements peuvent censurer les contenus et informations qu'ils désapprouvent, parfois sous couvert de la protection de la sécurité nationale, comme en témoigne cette déclaration de l'ancien ministre des Postes et Télécommunications chinois : *« Il s'agit d'adopter des mesures contre ce qui peut être préjudiciable à la sécurité du pays et irait à l'encontre des traditions chinoises »*[183]. À ce titre, la Chine a déployé l'un des systèmes les plus sophistiqués pour contrôler l'information sur Internet, en adoptant des systèmes de filtrage permettant de bloquer l'accès aux sites contenant des termes clés comme « démocratie » et « droits de l'homme »[184]. D'autres pays comme la Russie, l'Iran ou la Corée du Nord disposent également de systèmes de censure et de surveillance d'Internet très poussés, visant à réprimer les voix dissidentes et maintenir un contrôle strict des flux d'informations. Ainsi, en bloquant ou en filtrant des contenus sans respecter les critères mentionnés précédemment, les États méconnaissent le droit à la liberté d'expression : premièrement, les conditions spécifiques justifiant le blocage ne sont souvent pas prévues par la loi, ou le sont de manière trop large et vague, risquant un blocage arbitraire et abusif des contenus. Les listes de sites bloqués sont généralement tenues confidentielles, ne permettant pas d'évaluer si l'accès est limité pour des raisons légitimes. Deuxièmement, le blocage ne répond pas toujours aux objectifs énumérés à l'article 19.3 du Pacte international relatif aux droits civils et politiques[185]. Enfin, le blocage des

[180] Leloup, D., Untersinger, M., & Reynaud, F. (2015). L'impossible censure des sites pornographiques. *Le Monde.* https://www.lemonde.fr/pixels/article/2015/08/04/une-breve-histoire-de-la-censure-des-sites-pornographiques_4711451_4408996.html.

[181] La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[182] Anonyme. (2011). Les nouveaux médias : entre révolution et répression, la solidarité sur le Net face à la censure. *Reporters sans frontières*. https://rsf.org/fr/les-nouveaux-m%C3%A9dias-entre-r%C3%A9volution-et-r%C3%A9pression-la-solidarit%C3%A9-sur-le-net-face-%C3%A0-la-censure.

[183] Cité par Dominique Colomb, D., Mattelart, T. (2002). *La Mondialisation des médias contre la censure*. Ina et De Boeck, p. 289.

[184] Ibid.

[185] À savoir, le respect des droits ou de la réputation d'autrui ; la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques.

contenus se fait souvent sans intervention ou examen préalable d'une autorité judiciaire ou d'un organe indépendant. Dans son arrêt *Ahmet Yıldırım c. Turquie* de 2012, la CEDH a jugé que le blocage généralisé d'un site Web par les autorités turques constituait une violation de la liberté d'expression[186]. La Cour a précisé que les mesures de blocage doivent être strictement ciblées et proportionnées pour être conformes aux droits humains. Plus récemment, dans l'arrêt *Danilet c. Roumanie* du 20 février 2024, la CEDH a réaffirmé la protection de la liberté d'expression sur Internet, ainsi que la nécessité de préserver l'indépendance des institutions d'un État démocratique[187]. En outre, l'affirmation de la souveraineté numérique ne peut se faire au détriment du respect de la liberté d'expression, comme l'a justement souligné Bastien le Querrec, juriste à la Quadrature du Net : *« Dans une démocratie, la fin ne peut pas toujours justifier les moyens »*[188].

[186] CEDH, 18 décembre 2012, *Ahmet Yildirim c/ Turquie*, n°3111/10.
[187] CEDH, 20 février 2024, *Danilet c/ Roumanie*, n° 16915/21.
[188] Bougerol, E. (2023). Un projet de loi pour renforcer la censure du web : Une perspective inquiétante pour la liberté d'expression. *Basta Media*. https://basta.media/Un-projet-de-loi-pour-renforcer-la-censure-du-web-Une-perspective-inquietante-pour-la-liberte-d-expression.

## Conclusion

**Portée limitée de la régulation de l'accès aux sites pornographiques.** Il en a été fait mention en introduction, la loi SREN traduit la volonté du gouvernement français à exercer un contrôle plus étroit sur l'accès des mineurs aux contenus pornographiques. Or, les contraintes découlant, d'une part, des exigences fixées par le législateur européen pour la réalisation du marché unique, et d'autre part, de la nature même d'Internet en tant qu'espace neutre, ouvert et accessible à tous, révèlent l'incapacité de l'État français à opérer un contrôle à la fois exhaustif et proportionné. D'abord, l'effectivité du mécanisme de vérification d'âge dépend largement de son acceptabilité sociale : en effet, un processus trop contraignant inciterait les internautes, même les plus jeunes, à contourner cette vérification, notamment par le biais de VPN gratuits qui sont aujourd'hui largement accessibles par les mineurs. En ce qui concerne les adultes, certains pourraient être réticents à fournir une preuve de leur âge, par crainte de profilage, par défiance envers les tiers vérificateurs (qu'il s'agisse d'organismes publics ou privés) ou simplement pour conserver un strict anonymat sur Internet. Ils pourraient d'ailleurs s'orienter vers d'autres sources de contenus pornographiques, tels que les réseaux sociaux : récemment, X (ex-Twitter) a officiellement autorisé la diffusion de contenus pornographiques sur sa plateforme[189], mais n'impose -pour l'instant- aucun filtrage des mineurs. Or, le gouvernement français est doublement incompétent pour contraindre une telle plateforme à vérifier l'âge de ses utilisateurs : non seulement la plateforme X est basée en Irlande, ce qui rendrait illicite son blocage en France au regard du principe du pays d'origine, mais surtout, elle fait partie des « très grandes plateformes » dont la régulation est une prérogative réservée à la Commission européenne. Par conséquent, le législateur français ne peut imposer le strict respect de ses lois qu'aux éditeurs et hébergeurs de sites implantés sur son territoire national, ce qui réduit considérablement la portée de la loi SREN dans le cyberespace. Les sites hébergés sur le territoire national, quant à eux, devront se conformer au référentiel technique de l'Arcom pour ne pas être déréférencés par les fournisseurs d'accès Internet. Or, les exigences de protection de la vie privée exposées dans le projet de référentiel reprennent fidèlement les dispositions du RGPD ; en ce sens, l'exercice de la souveraineté numérique en matière de régulation de l'accès aux sites pornographiques est subordonné au respect des fondamentaux communautaires.

[189] Graillot A. (2024). Contenus pornographiques autorisés sur X (ex-Twitter) : quelles sont les règles françaises et européennes en la matière ? *Public Sénat*. https://www.publicsenat.fr/actualites/societe/contenus-pornographiques-autorises-sur-x-ex-twitter-quelles-sont-les-regles-francaises-et-europeennes-en-la-matiere.

**Tentatives d'appropriation d'Internet.** Internet a été conçu comme un réseau décentralisé, ouvert et sans frontières. Toutefois, certains États ont entrepris des actions visant l'appropriation d'Internet, en vue d'exercer un contrôle exhaustif sur les activités en ligne et d'affirmer leur souveraineté numérique. Les stratégies d'appropriation vont du durcissement de la législation nationale à la prise de contrôle des infrastructures clés, en passant par la mise sous tutelle des fournisseurs d'accès. Certains États ont pris l'initiative de créer leurs propres réseaux nationaux alternatifs ; c'est notamment le cas de la Corée du Nord avec son réseau *Kwangmyong* depuis 2002, de la Birmanie depuis 2010 et de l'Iran depuis 2012[190]. Ces réseaux nationaux sont généralement fermés et contrôlés par les autorités étatiques, offrant un accès limité à certains contenus et services agréés. Ils permettent aux États de renforcer leur souveraineté numérique en exerçant un contrôle total sur les flux d'informations transitant sur leur territoire. Cependant, ces stratégies soulèvent des préoccupations quant au respect des droits fondamentaux, tels que la liberté d'expression et la vie privée, mais également au regard des risques de fragmentation d'Internet ; elles ont pour effet de diviser le cyberespace, en créant des « îlots » nationaux contrôlés par les autorités étatiques, menaçant ainsi l'intégrité et l'unicité d'Internet[191]. Au-delà du contrôle de l'accès aux sites pornographiques, cette tension entre souveraineté numérique des États et nature décentralisée d'Internet révèle les enjeux de gouvernance du cyberespace, et la conciliation des intérêts nationaux avec la philosophie propre à l'Internet.

**Perspectives de coopération européenne et internationale.** L'une des principales motivations pour lesquelles les éditeurs et hébergeurs de sites pornographiques résistent aux tentatives de régulation est strictement financière ; l'industrie du contenu pour adultes en ligne représente un marché lucratif, estimé à plusieurs milliards de dollars par an[192], et leur modèle économique repose largement sur l'engagement des utilisateurs et leur dépendance au contenu. Plus les utilisateurs passent de temps sur le site, plus ils sont exposés à la publicité, ce qui augmente les revenus publicitaires. Ainsi, en imposant des restrictions sur l'accessibilité aux sites pornographiques, les États risquent de réduire les revenus potentiels de ces géants du net. Par ailleurs, les exigences en matière de vérification de l'âge ou de filtrage des contenus pourraient augmenter leurs coûts opérationnels et réduire leurs marges bénéficiaires. Dès lors, ils peuvent choisir de ne pas coopérer avec les autorités ou de contourner les restrictions en

[190] Sénat. (2014). L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne. Rapport d'information n° 696 (2013-2014), tome I, page 133. https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf.
[191] Pohle, J. & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532
[192] Anonyme. (2024). Quel est le business model de Pornhub ? *PSDW.* https://pswd.fr/modele-economique-pornhub/#Un_modele_economique_base_sur_la_publicite.

déplaçant leurs activités vers des juridictions plus permissives, à la manière d'un *law shopping*. Face à ce constat, une approche supranationale et coopérative faciliterait la mise en œuvre de mesures techniques et opérationnelles coordonnées, comme le blocage d'accès à certains sites ou la suppression de contenus illégaux. Toutefois, les perspectives d'harmonisation à l'échelle supranationale sont limitées, car le degré de censure des contenus pornographiques varie considérablement en fonction des traditions culturelles, des valeurs sociétales et des interprétations des droits fondamentaux. De plus, certains États pourraient être réticents à céder une partie de leur autorité réglementaire à des instances supranationales, craignant une atteinte à leur souveraineté numérique. Ce phénomène met en lumière un certain paradoxe : d'un côté, la capacité des États à faire appliquer leurs lois dans le cyberespace constitue un véritable enjeu de souveraineté numérique ; de l'autre, la nature transfrontalière d'Internet et le respect des droits humains rendent inévitable une coopération internationale.

## Annexes

*Annexe 1 : Entretien avec Olivier Blazy, professeur en cryptographie et cybersécurité à Polytechnique et co-créateur du dispositif de vérification d'âge reposant sur une preuve à divulgation nulle de connaissance et une signature de groupe.*

**Vous avez récemment présenté les contours de votre solution lors d'un séminaire sur la gouvernance des technologies émergentes au Stanford Cyber Policy Center (retransmis et accessible sur YouTube). La plupart de mes questions portent sur votre présentation et sur les différentes sources auxquelles j'ai eu accès sur le sujet.**

**D'abord concernant les acteurs permettant le fonctionnement de ce système, il y a les sites pornographiques d'un côté, les services tiers de l'autre, et au-dessus d'eux, une autorité certificatrice chargée d'accréditer ces services tiers, c'est-à-dire leur donner l'autorisation d'exercer le rôle de vérificateur et de transmetteur de la preuve de l'âge. Pourrait-on imager que ces autorités jouent à la fois le rôle de certificateurs et de tiers vérificateur, comme par exemple France Connect ?**

**O.B. :** Oui, il est tout à fait envisageable qu'une autorité, même si elle n'est pas traditionnellement chargée de la gestion des identités, assume à la fois le rôle de certificatrice et de tiers vérificateur. Dans mon intervention, je n'ai pas mentionné France Connect pour éviter toute confusion, mais il est possible que tout service étatique, qu'il soit spécialisé ou non dans la vérification des identités, puisse endosser ces deux rôles. Par exemple, un service comme France Connect, bien qu'il ne soit pas initialement conçu pour ce type de vérification, pourrait être adapté pour fournir à la fois l'accréditation des services tiers et la transmission de la preuve de l'âge des utilisateurs.

**Donc si l'on envisage les différents types de services tiers, on pourrait avoir le choix entre des services étatiques et des services proposés par des entreprises privées ? Je pense notamment à Apple Wallet ou Amazon Identity Provider par exemple.**

**O.B. :** Pour l'instant, parmi les tiers intéressés pour jouer ce rôle, on compte des entreprises telles que Docapost et Orange. La question est de savoir à quel point l'Etat est prêt à déléguer ce genre de services à des entreprises privées ? L'impulsion qui a été donnée par le précédent Ministre du numérique était plutôt positive sur cette question, cela pourrait donc être possible,

d'où la nécessité d'avoir une autorité de certification étatique qui s'assure que les entreprises à qui on délègue sont dignes de confiance.

**Justement, concernant ce prérequis de fiabilité et de confidentialité, il me semble que cela soit déterminant dans l'acceptation sociale de la solution. Si l'on envisage un service numérique de l'Etat, il faut que celui-ci soit perçu comme fiable, et la fuite de données de France Travail récemment ne met pas forcément en avant l'idée d'un service étatique très fiable. A votre avis, les utilisateurs seraient-ils davantage enclins à passer par un service tiers étatique ou par un service proposé par une entreprise privée ?**

**O.B. :** Je suis tout à fait d'accord, il y a beaucoup de services étatiques qui se sont fait piratés dernièrement et c'est une catastrophe, surtout lorsqu'on se penche sur les raisons de ces piratages, car la plupart du temps les recommandations de l'ANSSI n'ont pas été appliquées. Il y a beaucoup de choses qui pourraient être bien faites au niveau étatique, mais dans l'idée, France Connect existe déjà et a déjà accès à toutes nos données sensibles, donc les risques de piratage ne seraient pas augmentés. Par rapport à la façon dont on a conçu notre protocole, France Connect n'a aucun moyen de savoir quels sont les sites auxquels on essaie d'accéder, donc il n'y aurait pas d'informations supplémentaires qui leurs seraient transmises à ce niveau-là. On a vraiment dessiné notre protocole en faisant en sorte qu'aucune information supplémentaire ne transite, pour garantir la protection des données avec l'intervention de n'importe quel service tiers, qu'il soit étatique ou non. Maintenant, il est vrai que certaines personnes auront davantage confiance dans les entreprises privées, et cet enjeu de confiance est crucial, donc il faut permettre aux citoyens de choisir l'acteur qu'ils préfèrent. Toutefois, il semble que France Connect n'ait pas particulièrement envie d'être impliqué dans le processus de vérification d'âge.

**L'une de mes interrogations concerne l'aspect « stigmatisant » dans le simple fait de demander une preuve d'âge à un service, tel que notre banque par exemple. L'une des solutions envisagées pour prouver sa majorité était celle de « codes uniques de connexion » distribués en physique dans les bureaux de tabac, et la CNIL a considéré que cette solution était trop stigmatisante. Je sais que votre solution a vocation à être utilisée à d'autres fins, telle que l'inscription sur les réseaux sociaux ou la vente d'alcool en ligne**

**par exemple. Mais si, pour l'instant, cette solution est uniquement utilisée pour accéder aux sites pornographiques, n'y a-t-il pas un risque de stigmatisation ?**

**O.B. :** C'est justement là où il faudra faire très attention à encadrer ce que les vérifieurs peuvent faire de la collecte de données. L'Arcom a fait une consultation publique qui s'est récemment terminée, et parmi les remarques que j'ai faites, il y a celle de veiller à faire attention lorsqu'on utilise les banques : il ne faut pas que celles-ci puissent prendre en compte le nombre de requêtes qu'un utilisateur a généré pour accéder à des sites pour adultes, dans un but quelconque et notamment pour la gestion des crédits par exemple. Donc à ce niveau-là, il est nécessaire qu'un contrôle très poussé soit fait, et qu'il soit clairement visible pour les utilisateurs, afin de leur assurer que le nombre de requêtes ne soit pas utilisé à d'autres fins. Mais effectivement, cela sera assez stigmatisant, et je ne vois pas de façon de l'empêcher. On peut espérer que le fait que la requête soit numérique et de ne pas avoir à se présenter physiquement comme chez un buraliste encouragera -ou découragera moins- les personnes à jouer le jeu, mais l'on sait aussi que les traces numériques restent beaucoup plus longtemps.

**Concernant le coût de la vérification en elle-même, vous avez évoqué des montants allant d'un centime d'euro à plus d'un euro selon les solutions de vérification choisies par les sites. Ce coût serait-il supporté par les hébergeurs de sites pornographiques ou par les utilisateurs du site ?**

**O.B. :** Il s'agit des coûts actuels que facturent les services de vérification, qui sont généralement supportés par les sites. Si une plateforme veut faire une vérification de type « reconnaissance faciale » par exemple, elle paiera un forfait correspondant à 50 centimes ou 1 euro par vérification. Dans l'idéal, ce coût ne serait pas répercuté sur l'utilisateur. L'un des enjeux était donc de trouver un mécanisme avec la CNIL, par lequel on pourra continuer à faire cette facturation, malgré le fait que tout soit anonyme, et que les plateformes ne puissent pas savoir quel site a effectué la vérification.

**Vous avez précisé que les tiers vérificateurs allaient facturer leurs services tous les trois mois environ pour des raisons de protection de l'anonymat ?**

**O.B. :** Oui, la solution que l'on propose avec la CNIL est celle de ne pas avoir à payer « à la demande », c'est-à-dire pour chaque connexion d'un utilisateur sur la plateforme, car cela serait trop compliqué et menacerait l'anonymat des utilisateurs. Il y aurait ainsi un service étatique qui, tous les trois mois, effectuerait un contrôle, et listerait le nombre de tokens générés ainsi que leur provenance, afin de fixer le montant de la facturation. Cela permettrait d'avoir un mécanisme régulier de paiement, mais qui préserverait l'anonymat, en évitant les risques de liens ou de recoupement entre l'utilisateur et le service utilisé, et entre le service et le site.

**Sur le plan technique, comment pourrait-on s'assurer que les certificats de majorité, les preuves d'âge ne seront pas données ou vendues ?**

**O.B. :** Malheureusement, on ne peut pas tout à fait s'en assurer. Pour limiter ce risque, on a mis en place un système à usage unique : il y aura une sorte de numéro de série, un « challenge » généré par la plateforme, et on ne pourra utiliser un token que vis-à-vis de ce challenge, donc une seule fois. On pourrait toutefois imaginer un « commerce » où une personne, en essayant d'accéder à un site Web, va recevoir un challenge, passer par un service tiers pour générer le token, mais l'idée est que ce soit contraignant pour l'utilisateur car il devrait payer à chaque fois, ce qui, probablement, découragera énormément de mineurs de le faire. Le but est d'essayer de mettre un filtre au maximum.

**Et serait-il possible d'envisager un délai, d'avoir un certificat dont l'utilisation serait limitée dans le temps ?**

**O.B. :** Oui, mais c'est un élément qui devra être géré par les plateformes. Etant donné que certaines plateformes gèrent des millions de connexion sur des plages horaires assez limitées, les challenges qu'elles génèrent ne seront pas valides très longtemps, car cela impliquerait de les garder en mémoire. Le référentiel de l'Arcom préconise une durée d'une heure pour la vérification d'âge. On pourra donc parfaitement imaginer que ce challenge ait une durée de vie limitée de sorte à ce qu'il ne puisse pas être utilisé dans le temps.

**Concernant l'une des solutions proposées, qui serait le scan de la carte d'identité, vous avez évoqué lors de votre intervention qu'il sera nécessaire d'avoir une carte « locale »,**

**donc en l'occurrence une carte d'identité française, ce qui soulève notamment le problème des touristes ?**

**O.B. :** Oui, par exemple si un touriste ghanéen vient en France, et qu'il souhaite accéder à un site pour adultes, il devra malgré tout prouver qu'il est majeur. Pour cela, sa seule pièce d'identité sera son passeport ghanéen, donc il faut que la personne ou l'intelligence artificielle qui analyse l'image soit compatible avec les passeports de tous les pays du monde. Ce n'est pas impossible à mettre en place, mais il faut connaître les spécificités de tous les pays, et être à jour des normes et des potentielles nouvelles versions des documents d'identités. Il faut donc que la machine soit compatible, ce qui ne sera pas forcément aussi trivial et aussi automatique que l'analyse d'une carte d'identité locale. C'est un problème car le but lorsqu'on met ce genre de solution en place, c'est qu'elle ne soit pas discriminante envers certaines catégories de personnes, il faut vraiment faire attention à ne pas exclure les touristes.

**Donc à l'inverse, si un Français va à l'étranger, il n'aura pas du tout cette barrière de vérification, ce qui signifie que cette vérification est localisée, territorialisée ?**

**O.B. :** Exactement.

**Il est donc possible de mettre en place des mesures applicables dans un cyberespace « national » ?**

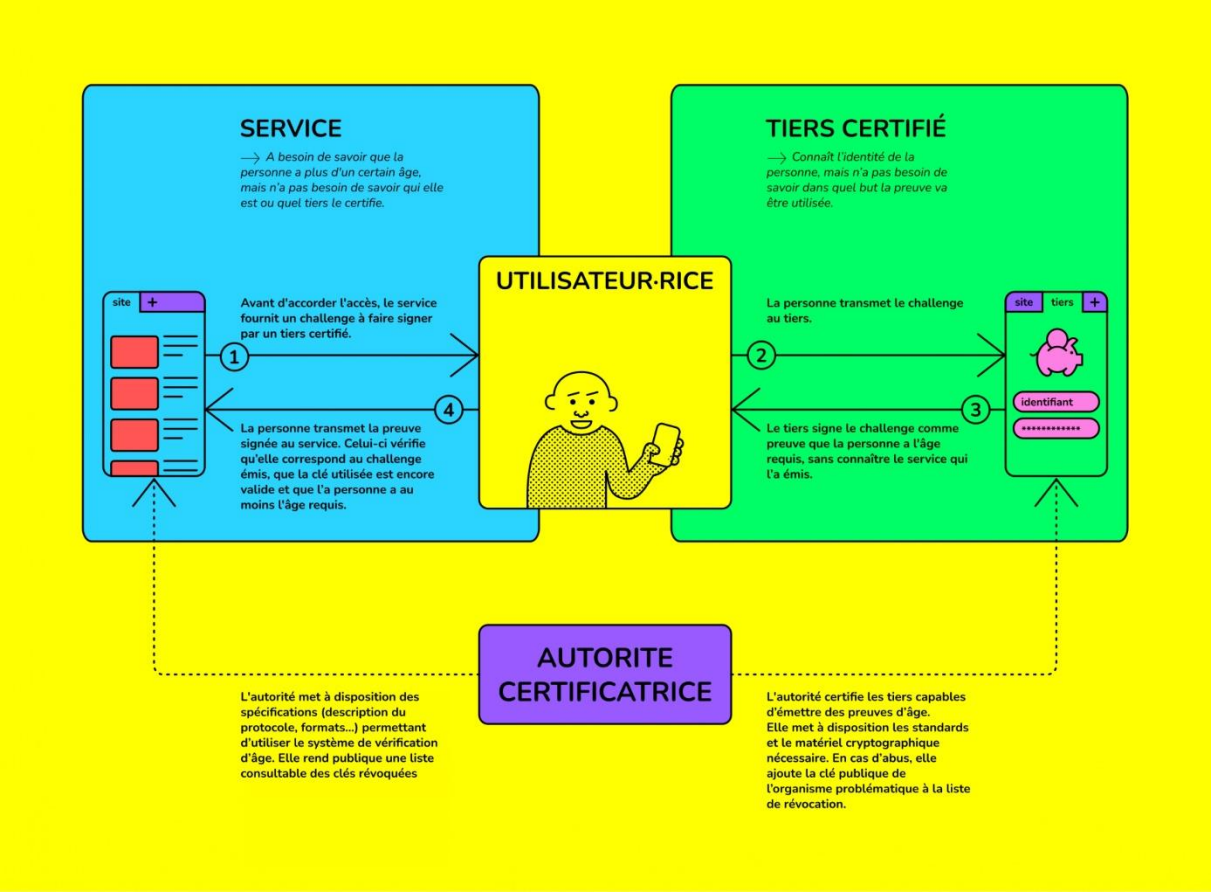
**O.B. :** D'un point de vue technique, ce n'est pas impossible, car une connexion est rattachée à une adresse IP, ce qui permet de vous localiser -plus ou moins-, de vous identifier et de voir quel fournisseur d'accès vous utilisez. A partir de cette adresse IP, on peut tout à fait retrouver le pays. Par exemple, votre adresse IP va indiquer que vous utilisez Orange, et sera localisée au centre d'Orange de Poitiers : lorsque vous vous connectez sur un site, il sait que vous êtes en France et va donc appliquer la législation française. Donc oui, sur le principe, il est possible de mettre en place des mesures sur l'internet français, mais l'utilisation d'un VPN permet de masquer le fait que vous êtes en France.

**Justement, sur l'utilisation d'un VPN, c'est un outil de contournement qui est facilement accessible, et vous avez déclaré qu'à votre avis, il ne faut pas les interdire, notamment**

**pour des raisons de sécurité. J'ai toujours considéré les VPN comme un outil assez peu sécurisé, puisqu'ils peuvent collecter nos données de navigation.**

**O.B. :** Un VPN, en soit, c'est simplement un outil qui permet de créer un réseau privé virtuel, donc de vous « mettre sur un autre réseau ». Beaucoup d'entreprises ont des solutions qui permettent d'accéder à leur propre réseau, ce qui est très sécurisé puisque seule l'entreprise a accès aux données transmises via le VPN. En revanche, effectivement, en utilisant les VPN gratuits ou les solutions commerciales pour les particuliers, on se retrouve sur le réseau de la société qui nous vend le VPN, et cette société aura accès à vos données personnelles, vos données de connexion et -au moins sur un VPN gratuit- risque de les réutiliser ou les revendre. Mais le fait d'interdire les VPN, en plus de pénaliser les entreprises et bloquer les intérêts nationaux, empêcherait les salariés de faire du télétravail de façon sécurisée, que cela soit dans les services de l'Etat ou dans les entreprises. De même, les voyageurs commerciaux venant de l'étranger ne pourraient pas venir en France pour travailler. Toutes ces conséquences se répercuteraient sur l'économie française.

*Annexe 2 : Schéma du fonctionnement technique du mécanisme de double anonymat*




*Source : Laboratoire d'Innovation Numérique de la CNIL. (2022). Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée. https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee*

# Bibliographie

## Ouvrages

Cattaruzza, A. & Buisson, J. (2023). *La Cyberdéfense. Politique de l'espace numérique.* Paris, Armand Colin, « Collection U », p. 57-65. https://www.cairn.info/la-cyberdefense--9782200634223-page-57.htm.

Delesse, C. (2016). *NSA National Security Agency. L'histoire de la plus secrète des agences de renseignement*, sous la direction de DELESSE Claude. Paris, Tallandier, « Hors collection », p. 325-329. https://www.cairn.info/nsa-national-security-agency--9791021008632-page-325.htm.

Mattelart, T. (2002) *La relation équivoque de la Chine avec Internet*. La Mondialisation des médias contre la censure, Ina et De Boeck, p. 289.

## Thèses et monographies

Leary, MG. (2022). *§230 of the Communications Decency Act: Regarding Child Sexual Abuse Material - The Experiment is Done and it Failed.* CUA Columbus School of Law Legal Studies. https://ssrn.com/abstract=4254010.

Renaissance numérique. (2022). *Contrôle de l'âge en ligne : pour une approche proportionnée et européenne.* https://www.renaissancenumerique.org/wp-content/uploads/2022/09/renaissancenumerique_controleage_rapport.pdf.

Levallois-Barth, C., Laurent, M. (2024). *Les acteurs de l'écosystème technique relatif aux identités numériques – Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique*. Chaire Valeurs et Politiques des Informations Personnelles. Institut Mines-Telecom. https://cvpip.wp.imt.fr/files/2024/02/2024-01-C-LEVALLOIS-M-LAURENT-acteurs-identites-numeriques.pdf.

Richter, A. (2021). *La réglementation des médias sociaux en Russie*. IRIS Extra, Observatoire européen de l'audiovisuel. https://rm.coe.int/iris-extra-2021fr-reglementation-des-medias-sociaux-en-russie/1680a3f8c7.

**Articles de presse**


Anonyme. (2021). Apple teams up with TSA to enable digital identification at security checkpoints. *Future Travel experience.* https://bit.ly/4aTXXF6.

Anonyme. (2023). How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. https://www.usenix.org/system/files/sec23fall-prepub-234-wu-mingshi.pdf.

Anonyme. (2024). Quel est le business model de Pornhub ? PSDW. https://pswd.fr/modele-economique-pornhub/#Un_modele_economique_base_sur_la_publicite.

Anonyme. (2023). Sites pornographiques : l'Australie abandonne son projet de vérification de l'âge des internautes. *Le Monde*. https://bit.ly/3yKztAJ.

Anonyme. (2023). Sites pornographiques : une demande de blocage renvoyée devant la cour d'appel. *Le Monde*. https://www.lemonde.fr/pixels/article/2023/10/18/sites-pornographiques-une-demande-de-blocage-renvoyee-devant-la-cour-d-appel_6195243_4408996.html.

Anonyme. (2023). Sites pornos : le système de vérification d'âge du gouvernement testé en mars. *Le Parisien avec AFP.* https://www.leparisien.fr/societe/sites-pornos-le-systeme-de-verification-dage-du-gouvernement-teste-en-mars-14-02-2023-PD6YYMDSJJDRZEPFJPQ7BAQFZQ.php.

Bougerol, E. (2023). Un projet de loi pour renforcer la censure du web : Une perspective inquiétante pour la liberté d'expression. Basta Media. https://basta.media/Un-projet-de-loi-pour-renforcer-la-censure-du-web-Une-perspective-inquietante-pour-la-liberte-d-expression.

Elegant, S. (2009). Chinese Government Attacks Google Over Internet Porn. *Time.* https://time.com/archive/6947092/chinese-government-attacks-google-over-internet-porn/.

Graillot A. (2024). Contenus pornographiques autorisés sur X (ex-Twitter) : quelles sont les règles françaises et européennes en la matière ? *Public Sénat.* https://www.publicsenat.fr/actualites/societe/contenus-pornographiques-autorises-sur-x-ex-twitter-quelles-sont-les-regles-francaises-et-europeennes-en-la-matiere.

Jerome, E. (2023). Le Turkménistan veut créer son propre réseau Internet coupé du monde. *Novastan.* https://bit.ly/4c7gnDq.

Legrand, D. (2020). DNS over HTTPS (DoH) : au-delà de Firefox, une « question de confiance ». https://next.ink/6139/108770-dns-over-https-au-dela-firefox-question-confiance/.

Leloup, D., Untersinger, M., & Reynaud, F. (2015). L'impossible censure des sites pornographiques. *Le Monde.* https://www.lemonde.fr/pixels/article/2015/08/04/une-breve-histoire-de-la-censure-des-sites-pornographiques_4711451_4408996.html.

Leloup, D. (2019). Comment un projet britannique de filtrage du porno a tourné à la catastrophe. *Le Monde.* https://www.lemonde.fr/pixels/article/2019/07/13/le-filtrage-du-porno-brxit-un-projet-britannique-qui-a-tourne-a-la-catastrophe-industrielle_5488904_4408996.html.

Le Priol, M. (2024). Numérique : la France accusée d'empiéter sur le droit européen. *La Croix*. https://www.la-croix.com/france/numerique-la-france-accusee-d-empieter-sur-le-droit-europeen-20240125.

Lucas, E. (2022). Blocage des sites pornographiques : la lutte de David contre Goliath. *La Croix.* https://www.la-croix.com/France/Blocage-sites-pornographiques-lutte-David-contre-Goliath-2022-10-04-1201236064.

Madelaine, N. (2013). Louis Pouzin : "L'Internet doit être refait de fond en comble", *Les Échos*, n°21442, p. 23.

Nocetti, J. (2019). La Russie en quête de son « Internet souverain ». *La revue des médias.* https://larevuedesmedias.ina.fr/la-russie-en-quete-de-son-internet-souverain.

Piquard, A. & Reynaud, F. (2023). Numérique : les projets de loi français accusés d'empiéter sur le droit européen. *Le Monde.* https://www.lemonde.fr/pixels/article/2023/11/09/numerique-les-projets-de-loi-francais-accuses-d-empieter-sur-le-droit-europeen_6199179_4408996.html.

Smaniotto, B. (2023). Pornographie : quels impacts sur la sexualité adolescente ? *The Conversation.* https://theconversation.com/pornographie-quels-impacts-sur-la-sexualite-adolescente-207142.

**Articles de revue**

Arifon, O. (2009). Les diverses facettes du contrôle d'Internet en Chine. Hermès, La Revue, 2009/3 (n° 55), p. 155-158. https://www.cairn.info/revue-hermes-la-revue-2009-3-page-155.htm.

Bellanger, P. (2015). Souveraineté numérique et ordre public. Archives de philosophie du droit, 2015/1 (Tome 58), p. 285-296. https://www.cairn.info/revue-archives-de-philosophie-du-droit-2015-1-page-285.htm.

Buolamwini, J., Gebru, T. (2018). Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91.

Douzet, F. (2014). La géopolitique pour comprendre le cyberespace. *Hérodote*, 152-153, 3-21. https://doi.org/10.3917/her.152.0003.

Dross, N. (2020). Fiche 7. La libre circulation des services ». Fiches de Politiques économiques européennes. Rappels de cours et exercices corrigés, sous la direction de DROSS Nicolas. *Ellipses*, p. 49-57. https://www.cairn.info/fiches-de-politiques-economiques-europeennes--9782340038387-page-49.htm.

Ghozlan, S. (2023). Blocage et déréférencement des "sites miroirs" – analyse du décret du 12 juin 2023. *Village de la Justice*. https://bit.ly/4c3Arqf.

Groffe-Charrier, J. (2023). Contenus pornographiques - Contrôle de l'âge du public de contenus pornographiques : l'ouverture de la boîte de Pandore ? *Communication Commerce électronique* n° 9, étude 18.

Harrel, Y. (2021). Comparatif des cyberpuissances : Etats-Unis, Chine, Russie » ? *Revue Conflits.* https://www.revueconflits.com/comparatif-cyberpuissances/.

Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions,* 30, 141-149. https://doi.org/10.3917/infle.030.0141.

Léon, A. (2023). Blocage et déréférencement des sites miroirs : l'autorité compétente désignée par décret. *Lexbase.* https://www.lexbase.fr/article-juridique/96835775-brevesblocageetdereferencementdessitesmiroirslautoritecompetentedesigneepardecret.

Marino, L. (2016). Responsabilité civile et pénale des fournisseurs d'accès et d'hébergement. Juris-Classeur Communication, fasc. n° 670, 1re éd. 2016.

Robin, A. (2024). Chronique de droit de l'internet. La Semaine Juridique Entreprise et Affaires n° 04.

**Rapports, avis et publications institutionnelles**

***Droit interne***

Arcom. (2023). Blocage des sites miroirs : une coopération prometteuse entre l'Arcom et les ayants droit de l'audiovisuel pour renforcer la lutte contre le piratage. https://bit.ly/3X9r4AY.

Arcom. (2024). Consultation publique sur le projet de référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques. https://www.arcom.fr/vos-services-par-media/consultations-publiques/consultation-publique-sur-le-projet-de-referentiel-determinant-les-exigences-techniques-minimales-applicables-aux-systemes-de-verification-de-lage-mis-en-place-pour-acces-contenus-pornographiques-en-ligne.

Arcom. (2023). Fréquentation des sites adultes par les mineurs. https://www.arcom.fr/nos-ressources/etudes-et-donnees/mediatheque/frequentation-des-sites-adultes-par-les-mineurs.

CNIL. (2021). Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée. https://www.cnil.fr/fr/controle-de-lage-sur-les-sites-web-la-cnil-invite-developper-des-solutions-plus-efficaces-et.

CNIL. (2024). France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger. https://www.cnil.fr/fr/france-travail-la-cnil-enquete-sur-la-fuite-de-donnees-et-donne-des-conseils-pour-se-proteger.

CNIL. (2022). Vérification de l'âge en ligne : trouver l'équilibre entre protection des mineurs et respect de la vie privée. https://www.cnil.fr/fr/verification-de-lage-en-ligne-trouver-lequilibre-entre-protection-des-mineurs-et-respect-de-la-vie.

Communiqué de presse du Conseil constitutionnel. Décision n° 2024-866 DC du 17 mai 2024. https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2024-866-dc-du-17-mai-2024-communique-de-presse.

Conseil d'Etat. (2024). Accès en ligne aux contenus pornographiques : le Conseil d'État saisit la Cour de justice de l'Union européenne de l'enjeu de la protection des mineurs. https://www.conseil-etat.fr/actualites/acces-en-ligne-aux-contenus-pornographiques-le-

conseil-d-etat-saisit-la-cour-de-justice-de-l-union-europeenne-de-l-enjeu-de-la-protection-des-min.

Laboratoire d'Innovation Numérique de la CNIL. (2022). Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée. https://linc.cnil.fr/demonstrateur-du-mecanisme-de-verification-de-lage-respectueux-de-la-vie-privee.

Laboratoire d'Innovation Numérique de la CNIL. (2023). Vérification de l'âge : l'argument économique. https://linc.cnil.fr/suite-demonstrateur-verification-de-lage-largument-economique-0.

Pôle d'expertise de la régulation numérique. (2022). Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? page 7. https://www.peren.gouv.fr/rapports/2022-05-20%20-%20Eclairage-sur-detection-mineurs_FR.pdf.

Sénat. (2014). Amendement présenté par Mme Nathalie GOULET et M. NAVARRO dans le cadre du Projet de loi relatif à la lutte contre le terrorisme. https://www.senat.fr/amendements/2014-2015/10/Amdt_1.html.

Sénat. (2019). Le devoir de souveraineté numérique. Rapport n° 7 (2019-2020), tome I. https://www.senat.fr/rap/r19-007-1/r19-007-1_mono.html.

Sénat. (2014). L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne. Rapport d'information n° 696 (2013-2014), tome I, page 133. https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf.

Sénat. (2022). Porno : l'enfer du décor. Rapport d'information n° 900 (2021-2022), tome I. https://www.senat.fr/rap/r21-900-1/r21-900-12.html.

***Common law***

British Standards Institution. (2018). Online age checking. Provision and use of online age check services. Code of Practice. https://shop.bsigroup.com/products/online-age-checking-provision-anduse-of-online-age-check-services-code-of-practice/standard/preview.

OFCOM. (2023). Guidance for service providers publishing pornographic content, page 17. https://www.ofcom.org.uk/__data/assets/pdf_file/0017/272600/consultation-part-5-guidance.pdf.

Walsh, M. & Woods, L. (2024). Response to Ofcom's consultation on guidance for providers publishing pornographic content. *Online Safety Act Network*. https://www.onlinesafetyact.net/analysis/response-to-ofcom-s-guidance-for-providers-publishing-pornographic-content/

***Droit de l'UE***

Commission européenne. (2021). Décision d'adéquation constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D1773&from=EN.

Commission européenne. (2020). Discours sur l'état de l'Union de la présidente von der Leyen en session plénière du Parlement européen. https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_20_1655.

Commission européenne. (2023). La Commission désigne une deuxième série de très grandes plateformes en ligne au titre du règlement sur les services numériques. https://ec.europa.eu/commission/presscorner/detail/fr/IP_23_6763.

European Union Agency for Fundamental Rights. (2022). Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi, page 8. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_fr.pdf.

Groupe de travail « article 29 » sur la protection des données. (2012). Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles », 00727/12/EN, WP 192, page 2. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_fr.pdf.

Parlement européen. (1997). Rapport sur la communication de la Commission sur le contenu illégal et préjudiciable sur le réseau Internet (COM(96)0487 - C4-0592/96). https://www.europarl.europa.eu/doceo/document/A-4-1997-0098_FR.html.

Parlement européen. (2023). Rapport de la commission des libertés publiques et des affaires intérieures sur la pornographie, PE 204.502/déf.

Parlement européen et Conseil de l'UE, (2024). Proposition de règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401183.

Projet de résolution législative du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique (Doc. COM (2021)0281 – C9-0200/2021 – 2021/0136(COD)).

***Droit international***

Assemblée parlementaire du Conseil de l'Europe. (2022). Pour une évaluation des moyens et des dispositifs de lutte contre l'exposition des enfants aux contenus pornographiques », Rapport | Doc. 15494. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=29890&lang=fr.

Grother, P., Ngan, M. & Hanaoka, K. (2018). Ongoing Face Recognition Vendor Test, part 1., National Institute of Standards and Technology. https://www.congress.gov/116/meeting/house/109578/documents/HHRG-116-GO00-20190604-SD008.pdf.

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council. https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

**Délibérations**

CNIL. (2021). Délibération n° 2021-069 du 3 juin 2021 portant avis sur un projet de décret relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

**Normes**

***Droit interne***

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».

Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique.

Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

***Droit de l'UE***

Règlement 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE.

Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

**Jurisprudences**

***Droit interne***

Conseil constitutionnel, Décision n° 2024-866 DC du 17 mai 2024.

Cass. Civ. 1ère, 18 oct. 2023, n° 22-18.926.

Cass. 1re civ., 5 janv. 2023, n° 22-40.017.

***Droit de l'UE***

CJUE, *Inspektor v Inspektorata kam Visshia sadeben savet*, 8 déc. 2022, aff. C-180/21.

***Droit international***

CEDH, *Ahmet Yildirim c/ Turquie*, 18 déc. 2012, n°3111/10.

CEDH, *Danilet c/ Roumanie*, 20 fév. 2024, n° 16915/21.