Le Centre d'Études Jacques Georgin est un centre d'éducation permanente reconnu par la Fédération Wallonie-Bruxelles
ASBL Centre d'Études Jacques Georgin – 127, Chaussée de Charleroi à 1060 Bruxelles
N° d'entreprise : 0412.759.942. – RPM : Tribunal de l'entreprise francophone de Bruxelles. BE30 7320 3232 6111

Note d'analyse 2 – 25 du Centre d'études Jacques Georgin

« Vers une fin de l'anonymat sur les réseaux sociaux pour combattre l'impunité ? »

Bruxelles, le 31 mars 2025

Christophe DUBOIS, Directeur du Centre d'études Jacques Georgin

Avant-propos

La présente note d'analyse du Centre d'études Jacques Georgin s'inscrit dans le prolongement d'entretiens menés avec plusieurs associations belges actives dans la lutte contre le cyberharcèlement parmi lesquelles **Child Focus**, **Infor Jeunes** et la **Ligue des droits humains**. Ces échanges ont permis de recueillir des témoignages concrets ainsi que des éclairages professionnels sur les mécanismes de harcèlement en ligne, les difficultés liées à l'identification des auteurs, et les limites actuelles des dispositifs juridiques. Un constat commun émerge de ces consultations : l'anonymat permis par les plateformes numériques, tout en constituant un vecteur de liberté d'expression, apparaît également comme un facteur facilitant la propagation de comportements malveillants, voire délictueux, en ligne.

Dans ce contexte, la question d'un encadrement plus strict, voire d'une remise en cause partielle de l'anonymat sur les réseaux sociaux, se pose avec acuité. L'objectif serait de mieux responsabiliser les utilisateurs tout en offrant aux victimes des moyens plus efficaces de protection et de recours. Néanmoins, cette perspective soulève des interrogations légitimes quant à la préservation des libertés fondamentales, en particulier celle de s'exprimer sans crainte de représailles. Cette note vise ainsi à analyser les enjeux juridiques, sociaux et éthiques liés à une éventuelle limitation de l'anonymat numérique, dans une optique de lutte contre l'impunité en ligne.

Le concept d'anonymat

La place proéminente des réseaux au sein de notre société induit le fait que le concept d'anonymat est naturellement lié au cyberespace. Au moment où le web voyait le jour, ce concept prenait la forme d'une promesse faite à ses utilisateurs. Ainsi, dans sa Déclaration d'indépendance du cyberespace, J.P. Bartlow écrivait : « Nos identités n'ont pas de corp, donc, contrairement à vous, nous ne pouvons pas obtenir l'ordre par coercition physique ».

Une définition de l'anonymat

Si nous avons tendance percevoir l'anonymat comme un état excluant toute possibilité d'identification, l'anonymat est toujours contextuel ou relationnel, en réalité. Dès lors, il n'est jamais complet, même dans les sociétés purement analogiques. Un auteur qui écrit un livre sous un pseudonyme ou de manière anonyme ne révèle pas son nom, son sexe ou sa nationalité au public. Néanmoins, il partage des idées ou des compétences, éléments qui font partie de son identité. De plus, un auteur peut construire son capital artistique sur la base de publications anonymes ou pseudonymes. Nous parlons, alors, d'une limitation ontologique profonde de l'anonymat.

Existe-t-il un moyen vraiment efficace de parvenir à l'anonymat, même sous cette forme limitée ? Si nous revenons à l'exemple de l'auteur anonyme, nous pouvons en utiliser les fragments connus de l'identité afin d'en décoder les éléments. En outre, plus une personne produit des écrits, plus il est facile d'en révéler l'ensemble du tableau. Cela est d'autant plus important que dans la réalité des réseaux sociaux, nous devons faire exclure des centaines de massages et d'autres activités qui, dans certains cas, peuvent être aussi importants pour révéler l'identité d'une personne. De surcroît, les méthodes sophistiquées d'acquisition et d'analyse de données dont disposent les entreprises de réseaux sociaux nous permettent de nous rendre compte que l'anonymat total relève de l'impossible dans la réalité des plateformes de réseaux sociaux.

1. L'anonymat comme fonctionnalité des plateformes

Les réseaux sociaux ne permettent pas réellement l'anonymat ; ils le fournissent comme une simple fonctionnalité. Ce phénomène est lié au concept de dissociabilité, où l'anonymat peut être analysé sous trois angles :

- **L'expéditeur et le destinataire** : peut-on relier un message à un utilisateur ?
- **La relation** : peut-on observer l'échange d'informations entre utilisateurs?

Les plateformes centralisées ont un contrôle total sur ce processus, puisqu'elles gèrent toute l'infrastructure, de l'envoi au traitement des données.

De plus, l'anonymat est contextuel : sur les réseaux sociaux, bien que les utilisateurs soient nombreux, leurs interactions ressemblent à celles de petites communautés. Cela signifie que l'échange d'informations est public et que la "distance" entre les individus est courte, facilitant la surveillance. Contrairement aux petits villages où l'autorégulation sociale protège la vie privée, le "village global" numérique expose ses membres sans véritable protection.

En conséquence, l'anonymat protège partiellement des autres utilisateurs mais pas des plateformes elles-mêmes ni des États. Les régimes autoritaires limitent déjà fortement l'anonymat en ligne, et même les pays démocratiques développent des outils sophistiqués pour surveiller et intercepter les communications, y compris celles des cybercriminels.

2. Les limites de l'anonymat sur les réseaux sociaux

Même les plateformes dites décentralisées (comme celles basées sur la blockchain) ne garantissent pas un anonymat absolu. La transparence inhérente à la blockchain[1] permet d'analyser les interactions stockées et d'identifier indirectement les utilisateurs.

Le texte propose donc une définition de l'anonymat en prenant en compte :

1. La définition classique où l'on ne peut être identifié au sein d'un ensemble.
2. Son caractère contextuel et relationnel, rendant l'anonymat absolu impossible.
3. Les obstacles croissants à l'anonymat : méta-analyse des données, dépendance aux plateformes, surveillance étatique.
4. La distinction entre anonymat et pseudonymat : les plateformes offrent du pseudonymat (utilisation de pseudonymes), mais pas un véritable anonymat.

3. L'identité numérique et son contrôle

L'identité numérique peut être vue comme :

- Une solution technique pour identifier quelqu'un en ligne.
- Un ensemble de données reflétant l'identité sociale d'un individu.

Notre identité en ligne est de moins en moins liée à notre nom réel et repose plutôt sur la perception des autres utilisateurs. Les plateformes influencent fortement cette identité en contrôlant les algorithmes et le contenu mis en avant, notamment chez les jeunes utilisateurs.

[1] Il s'agit d'une base de données distribuée, dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés, puis groupés à intervalles de temps réguliers en « blocs », lesquels forment ainsi une chaîne de plus en plus longue. L'ensemble est sécurisé par cryptographie.

Les solutions d'identité numérique sont encore principalement fournies par les plateformes, bien que des alternatives gouvernementales (comme l'initiative européenne) ou décentralisées émergent. Cependant, la centralisation et la connexion de plusieurs services sous une seule identité compliquent encore plus l'anonymat.

4. La protection de la vie privée

L'anonymat est souvent associé à la vie privée, mais leur relation varie selon les cultures juridiques :

- **En Europe** : la vie privée est liée à la dignité et à l'autodétermination informationnelle.
- **Aux États-Unis** : elle est davantage perçue comme un moyen de limiter l'ingérence de l'État.

La vie privée dépend de la difficulté à faire circuler l'information. L'essor des plateformes numériques a créé un nouvel écosystème où ces frictions sont réduites, facilitant la surveillance. Cependant, l'anonymat et le chiffrement restent des outils pour protéger la vie privée, malgré l'omniprésence des États et des entreprises dans la gestion des données personnelles.

5. Avantages et risques de l'anonymat sur les réseaux sociaux

À l'heure actuelle, l'anonymat englobe une interaction complexe entre divers domaines, notamment la vie privée, la responsabilité et la liberté d'expression dans les régimes démocratiques et non démocratiques. Dès lors, un examen approfondi des avantages et des risques de l'anonymat permet de bien comprendre ses implications et d'élaborer des recommandations politiques efficaces.

5.1. Avantages et opportunités

5.1.1. Garantie de la liberté d'expression

L'anonymat renforce considérablement la liberté d'expression. Il facilite les débats ouverts sur des sujets difficiles et protège ceux qui expriment des opinions dissidentes, surtout dans les régimes politiques autoritaires. D'une part, il incite les personnes à partager leurs avis sur les réseaux sociaux sans redouter de conséquences politiques ou personnelles, les encourageant à aborder des sujets qu'elles éviteraient autrement. Cela mène à un débat public plus varié et transparent, ce qui est positif pour les démocraties. D'autre part, à l'ère numérique où les groupes de lanceurs d'alerte et de militants se développent et où les réseaux sociaux sont clés pour diffuser des informations sensibles, l'anonymat est vital pour protéger ces acteurs des représailles. Le Printemps arabe en est un exemple marquant : des militants ont utilisé des comptes anonymes pour organiser des mouvements et informer sur la répression, tout en restant hors de portée des autorités.

5.1.2. Garantie de la protection de la vie privée

Dans un contexte actuel marqué par une inquiétude croissante concernant la collecte des informations personnelles et une redéfinition de la notion de vie privée, l'anonymat peut offrir des avantages importants aux utilisateurs en matière de protection de leur vie privée. Ainsi, la vie privée informationnelle ne se limite pas au contrôle des données personnelles, mais englobe également la volonté de préserver son identité et son indépendance.

L'utilisation de comptes anonymes sur les réseaux sociaux et les interactions en ligne peuvent protéger les utilisateurs d'une surveillance non désirée et leur permettre de restreindre la diffusion de leurs informations personnelles. Bien qu'un anonymat total et une protection complète contre l'identification par les réseaux sociaux soient illusoires, l'adoption de cette idée de traçabilité partielle permet aux utilisateurs d'éviter de laisser des traces de données personnelles qui pourraient être exploitées à des fins commerciales ou malveillantes, comme le vol d'identité.

De plus, l'anonymat établit une distinction entre les données de profil et les données comportementales, séparant les informations sensibles des utilisateurs – telles que le nom, l'adresse et la date de naissance – de leurs activités en ligne. Cela donne aux individus la possibilité de reprendre le contrôle des informations qu'ils préfèrent ne pas divulguer en ligne et diminue le risque d'un suivi malintentionné qui pourrait relier leurs actions à leur identité.

5.1.3. Divulgation de soi et santé mentale

Même si son étendue est plus limitée que la liberté d'expression et la protection de la vie privée, l'anonymat sur les réseaux sociaux s'est révélé crucial pour les personnes en quête de soutien concernant des sujets délicats et personnels, comme les problèmes de santé mentale, les dépendances ou les traumatismes.

En favorisant la confidence et en réduisant les inhibitions en ligne, l'anonymat permet aux utilisateurs d'exprimer leurs émotions, de solliciter des conseils et de partager leurs vécus sans redouter le jugement d'autrui ou des répercussions sociales défavorables. Des recherches ont mis en évidence l'effet bénéfique de cela sur le bien-être psychologique.

5.2. Risques et enjeux

L’anonymat sur les réseaux sociaux , malgré ses nombreux avantages, présente également plusieurs risques pour les utilisateurs . Cette analyse se concentre sur trois défis principaux, qui découlent tous d’une question clé : le manque de responsabilité.

5.2.1. Cyberintimidation et harcèlement

La large utilisation des réseaux sociaux, associée à l'anonymat, a facilité les interactions entre les utilisateurs, y compris des comportements tels que le harcèlement en ligne et la cyberintimidation. L'anonymat est un facteur favorisant la

cyberintimidation, car le manque d'informations permettant d'identifier les personnes encourage les utilisateurs à adopter des conduites nuisibles avec peu, voire pas de répercussions. De fait, il devient compliqué de retrouver l'auteur de ces actes. Ce manque de responsabilité peut créer un environnement en ligne malsain, où les utilisateurs se sentent plus enclins à adopter des comportements agressifs ou abusifs qu'ils n'auraient pas dans des interactions directes.

Par conséquent, l'ampleur et la fréquence élevées de la cyberintimidation peuvent engendrer une profonde souffrance psychologique chez les victimes, qui peuvent développer de l'anxiété, de la dépression, une faible estime de soi, et même des pensées suicidaires.

5.2.2. De la désinformation

L'anonymat sur les réseaux sociaux pose un défi majeur avec la propagation de fausses informations et de propagande trompeuse. Il offre un environnement favorable aux robots, aux faux profils et aux échanges non authentiques sur divers sujets, créant ainsi un écosystème d'information en ligne peu fiable et douteux, ce qui peut avoir des répercussions concrètes.

Les robots sur les réseaux sociaux, qui sont des comptes automatisés capables de générer du contenu et d'interagir avec de vrais utilisateurs, se développent dans un contexte qui valorise l'anonymat en ligne. Étant donné que beaucoup de personnes s'informent via les réseaux sociaux, ces robots jouent un rôle crucial dans l'orientation des discussions en diffusant de fausses nouvelles sur des sujets variés, allant de la politique à la santé. Ils sont programmés pour amplifier certains discours ou influencer l'opinion publique, manipulant ainsi les réseaux sociaux et trompant les utilisateurs dès le début, avant que le contenu ne devienne viral. Ils ciblent particulièrement l'interaction avec des utilisateurs influents par le biais de réponses et de mentions. Cette vulnérabilité à la manipulation est manifeste, car les individus ont tendance à retweeter les contenus peu fiables partagés par des robots presque aussi souvent que ceux partagés par d'autres personnes. Dans ce cas, on peut parler d'engagement irresponsable, car il est impossible d'identifier clairement l'identité de l'émetteur ou de savoir si le message provient d'une personne réelle. Enfin, l'anonymat offert par les plateformes de réseaux sociaux rend difficile de retrouver l'origine des créateurs de robots ou de les tenir responsables de la diffusion de fausses informations.

Cet environnement de désinformation en ligne engendre de nombreuses conséquences dans le monde réel, allant de la manipulation des campagnes électorales à la diffusion de fausses informations concernant des questions de santé publique.

6. Approches politiques et juridiques

6.1. Réglementations existantes sur l'anonymat

Pour de nombreux pays occidentaux, l'anonymat de l'identité et de la communication est un droit légal garanti par l'article sur la liberté d'expression de la Charte des droits de l'homme des Nations unies de 1948. Cependant, garantir l'anonymat est complexe parce que des limitations à la liberté d'expression et à l'anonymat peuvent être justifiées dans certaines circonstances pour des raisons telles que la sécurité nationale, la prévention de la diffamation, du harcèlement ou de l'incitation à la haine. Dans les pays dotés de systèmes médiatiques libéralisés, les défis liés à l'anonymat en ligne consistent souvent à trouver un équilibre entre les droits d'expression et les autres droits individuels dans le cadre de ce pseudo-anonymat ou de cet anonymat conditionnel.

6.1.1. Les régimes démocratiques

États-Unis et Amérique du Nord

Aux États-Unis, la Cour suprême accorde habituellement une protection aux discours anonymes en s'appuyant sur le premier amendement. Cependant, comme pour d'autres droits constitutionnels, elle met en balance cette protection avec d'autres intérêts, notamment dans les domaines de l'activité politique et du financement des campagnes électorales. Sur internet, la Cour suprême a reconnu le droit à l'anonymat dans les propos tenus, mais pas comme un droit absolu, et les tribunaux des États ont généralement adopté une position similaire.

En droit canadien, ce droit est parfois perçu comme étant lié au droit à la vie privée. Concernant l'anonymat en ligne, les tribunaux canadiens ont développé un critère d'équilibre. Ce critère exige que la partie qui cherche à identifier des utilisateurs anonymes prouve d'abord qu'elle a une requête légitime et qu'il n'existe pas d'autre moyen d'obtenir les informations nécessaires. Si cette preuve est apportée, le tribunal doit alors évaluer les éléments en faveur et en défaveur de la divulgation. Les tribunaux canadiens ont établi ce critère dans une affaire concernant une tentative de révéler l'identité des clients d'un fournisseur d'accès internet qui auraient enfreint les droits d'auteur du plaignant.

Royaume-Uni

En 1973, la Chambre des Lords a défini un ensemble de conditions pour qu'un plaignant puisse contraindre un tiers à révéler l'identité de potentiels défendeurs dans le cadre d'un procès. La partie qui sollicite ces informations doit prouver que la partie inconnue a probablement commis une faute à son encontre, que l'identification de cette partie est nécessaire, et que le tiers est capable de fournir l'identité de l'auteur présumé de la faute. Les tribunaux doivent évaluer les intérêts du tiers à maintenir la confidentialité et les impératifs de la justice. Ce critère a également été appliqué dans d'autres affaires judiciaires au Royaume-Uni concernant des forums internet et d'autres publications en ligne.

L’Union européenne

Le droit européen tend à offrir une protection de la vie privée plus étendue que le droit américain, bien que le niveau de cette protection puisse varier légèrement entre les pays. L'anonymat est parfois perçu comme un droit lié à la vie privée, notamment en ce qui concerne les informations personnelles. En 2003, le Comité des ministres du Conseil de l'Europe a abordé le principe de l'anonymat dans sa déclaration sur la liberté de communication sur Internet. Cette déclaration stipule que, pour assurer la protection contre la surveillance en ligne et renforcer la libre expression des informations et des idées, les États membres doivent respecter la volonté des internautes de ne pas dévoiler leur identité.

En 2013, le Parlement européen a voté en faveur d'une nouvelle réglementation obligeant les entreprises à anonymiser les données personnelles collectées auprès des utilisateurs. Cette décision a suivi l'insistance de la chancelière allemande Angela Merkel pour que les commissaires européens soutiennent une réglementation imposant aux entreprises du secteur internet d'indiquer à qui elles transmettent les informations personnelles des utilisateurs. En 2014, la Cour de justice de l'Union européenne a jugé que Google et d'autres fournisseurs de services et de contenu en ligne devaient, dans certaines situations, accepter les demandes de suppression d'anciens liens vers des informations, même exactes, concernant des individus, afin qu'elles n'apparaissent plus dans les résultats de recherche associés à ces personnes.

Plus récemment, depuis mai 2018, le Règlement général sur la protection des données (RGPD), une réglementation de l'UE concernant la protection des données et de la vie privée pour tous les individus au sein de l'Union européenne (UE), vise à donner aux citoyens un meilleur contrôle sur leurs données personnelles et à harmoniser les règles de protection des données au sein de l'UE. Il impose des exigences strictes sur la manière dont les données personnelles sont collectées, traitées et conservées, et accorde également aux individus le droit d'accéder à leurs données, de les rectifier et de les effacer dans certaines conditions. Il s'applique à toutes les organisations qui traitent des données personnelles, qu'elles soient établies à l'intérieur ou à l'extérieur de l'UE.

Concernant l'anonymat en ligne, le RGPD encourage l'utilisation de la pseudonymisation[2] et du chiffrement pour diminuer les risques pour les personnes concernées tout en aidant les responsables du traitement et les sous-traitants à respecter leurs obligations. La législation européenne exige des responsables du traitement qu'ils mettent en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, afin de respecter les principes de protection des données et d'intégrer les garanties nécessaires dans le traitement des données personnelles. Le règlement mentionne spécifiquement la pseudonymisation et le chiffrement comme des outils à utiliser par les responsables du traitement et les sous-traitants dans le cadre du traitement des données personnelles. Des législations européennes récentes, comme la loi sur les marchés numériques, qui vise à créer un marché numérique équitable et compétitif dans l'UE en régulant les « gatekeepers »[3], et la loi sur les services numériques, qui oblige les grandes plateformes en ligne à lutter contre la haine, les "fake news" et la criminalité sur internet, offrent la possibilité

de mettre en place des protections dans l'intérêt des personnes concernées. Celles-ci incluent également la pseudonymisation et l'anonymisation des données personnelles. Avec ces législations, l'anonymisation des données pourrait prendre de l'importance, mais le RGPD reste la référence en matière de traitement des données personnelles.

Il est important de noter qu'en vertu du RGPD, si les données personnelles sont correctement anonymisées, elles ne sont plus considérées comme telles, et par conséquent, les dispositions du RGPD relatives à la protection des données personnelles ne s'appliquent pas aux données anonymisées.

En conclusion, le droit à l'anonymat en ligne n'est pas explicitement mentionné comme un droit autonome dans la législation européenne. Néanmoins, certaines affaires relatives à l'anonymat en ligne portées devant la Cour européenne des droits de l'homme montrent que la Cour considère l'anonymat comme un élément essentiel de la protection de la liberté d'expression en ligne au sein de l'Union européenne. Le 7 décembre 2021, la Cour a rendu son arrêt dans l'affaire Standard Verlagsgesellschaft MBH c. Autriche (n° 3), concluant que le tribunal autrichien avait violé le droit à la liberté d'expression du requérant en lui demandant de révéler l'identité des personnes ayant publié des commentaires prétendument diffamatoires sur son site web.

6.2. Approches restrictives en matière d'anonymat en ligne

Dans les pays où les systèmes médiatiques sont restreints, l'anonymat en ligne peut être totalement interdit ou fortement limité par des lois et des règlements exigeant des fournisseurs d'accès à internet et des plateformes en lignes qu'ils collectent et conservent les données des utilisateurs, y compris leur identité et leurs activités en ligne. Ces données peuvent être utilisées par les agences gouvernementales pour surveiller et contrôler le contenu en ligne, et pour identifier et poursuivre les individus qui expriment des opinions dissidentes et s'engagent dans des activités jugées menaçantes pour le régime.

[2] Il s'agit d'un traitement de données à caractère personnel de manière qu'on ne puisse pas attribuer les données à une personne physique sans avoir recours à des informations supplémentaires.

[3] Les portiers (GK: Gatekeeper) sont des éléments optionnels dans une solution de réseau informatique H. 323. Ils ont pour rôle de réaliser la traduction d'adresse (numéro de téléphone - adresse IP) et la gestion des autorisations.

6.2.1. Les régimes autoritaires

La Russie

Le gouvernement russe a mis en place diverses mesures pour exercer un contrôle sur l'utilisation d'Internet par ses citoyens. La loi de 2006 sur « l'information, les technologies de l'information et la protection de l'information » impose aux fournisseurs de services en ligne de recueillir et de conserver certaines informations sur leurs utilisateurs, notamment leur nom complet, leur adresse et d'autres données permettant de les identifier. Les lois « Yarovaya » (2016) et sur « l'isolement de l'Internet » (2019) ont renforcé cette législation en exigeant des fournisseurs de services en ligne qu'ils installent des équipements permettant au gouvernement de bloquer l'accès à certains sites web et services, et qu'ils conservent des informations sur les activités en ligne des utilisateurs, telles que leur historique de navigation et leurs requêtes de recherche, pendant au moins six mois. De plus, il a été rapporté que le ministère russe de l'intérieur offrait près de 100 000 dollars pour des recherches sur les méthodes d'identification des utilisateurs anonymes de Tor, un réseau qui masque l'origine et la destination de la navigation sur Internet et empêche le suivi des utilisateurs.

La Chine

Bien que la Constitution chinoise garantisse les libertés d'expression, d'association et de publication sous l'autorité du parti au pouvoir, le gouvernement chinois a déployé des efforts considérables pour limiter l'anonymat et la participation à des sujets sensibles. Il a mis en place un système complexe de filtrage, de blocage et de surveillance des sites web, des fournisseurs d'accès à Internet et des utilisateurs. En 2011, 2012 et 2016, la Chine a adopté diverses mesures pour restreindre l'anonymat en ligne, notamment la création d'une nouvelle agence chargée de coordonner la régulation d'Internet, l'augmentation de la pression sur les intermédiaires pour qu'ils pratiquent l' « autocensure » des contenus et des utilisateurs, et le renforcement des contrôles sur les réseaux sociaux. En 2012, le gouvernement chinois a instauré une politique obligeant les internautes à s'enregistrer sous leur véritable identité auprès des fournisseurs de services, afin d'aider ces derniers à mieux protéger les informations de leurs clients. Enfin, pour clarifier la situation, la « loi sur la cybersécurité » et la « loi sur la sécurité de l'internet », promulguées en 2016 et 2017, exigent des fournisseurs de services en ligne qu'ils conservent les données collectées en Chine sur des serveurs situés dans le pays et qu'ils en accordent un accès total aux autorités gouvernementales sur demande. Ceci illustre clairement que le droit à l'anonymat en ligne n'est pas réellement garanti en Chine.

6.3. Approches politiques de la vérification d’identité

Face à l'augmentation du nombre d'abus et de harcèlements, et à l'essor des campagnes mondiales de désinformation rendues possibles par les réseaux de robots sur les réseaux sociaux, les régulateurs ont commencé à s'intéresser davantage à l'élaboration de politiques susceptibles d'endiguer ces comportements indésirables sur les réseaux sociaux. L'anonymat est souvent désigné comme le coupable de la

prévalence du harcèlement et des abus en ligne, car l'anonymat favorise les comportements antisociaux. Cela a conduit certains décideurs politiques à émettre des propositions visant à interdire ou à réglementer la possibilité pour les utilisateurs des plateformes de réseaux sociaux de préserver leur anonymat. Le Royaume-Uni et l'Australie ont examiné la possibilité d'imposer des exigences de vérification de l'identité pour l'ouverture de comptes de réseaux sociaux et un projet de loi au Sénat français a tenté de créer une autorité gouvernementale indépendante chargée de lier l'identité des utilisateurs français de réseaux sociaux à leurs comptes, interdisant de fait les comptes anonymes de réseaux sociaux (*Proposition de Loi Instituant une Autorité de Contrôle de l'identité Numérique*, 2021). Bien qu'aucune de ces propositions n'ait été mise en œuvre, car elles étaient considérées comme une entrave significative à la liberté d'expression, elles soulignent l'intérêt continu des décideurs politiques pour l'utilisation des mesures d'identification comme outil de dissuasion des abus en ligne. En effet, il est nécessaire de trouver un juste équilibre entre la liberté accordée aux utilisateurs de réseaux sociaux par l'anonymat et la mise en œuvre de mesures politiques permettant aux autorités compétentes de poursuivre efficacement les comportements illicites sur ces plateformes. En fonction de l'approche adoptée, ces politiques peuvent se situer sur différentes parties du spectre entre l'anonymat et le contrôle de l'activité de l'utilisateur.

6.3.1. Politique en matière de « nom réel »

La solution la plus extrême à ce problème serait de rendre obligatoire l'utilisation de la véritable identité des utilisateurs sur les plateformes de réseaux sociaux, interdisant ainsi l'usage de pseudonymes. Cette approche est déjà celle de certaines plateformes, comme Facebook avec sa politique du « vrai nom ». Cependant, cette mesure porte considérablement atteinte au droit des utilisateurs des réseaux sociaux d'agir sous des alias ou des pseudonymes dans leurs activités en ligne. Facebook a d'ailleurs dû assouplir sa propre politique face aux vives critiques des associations de défense des libertés civiles. Ce point de vue est partagé par plusieurs organismes de réglementation, notamment le Comité européen de protection des données et la CNIL en France, qui affirment que chaque utilisateur a le droit d'utiliser des pseudonymes et devrait être libre de posséder plusieurs identités numériques, dont les caractéristiques ne se recoupent pas nécessairement et qui peuvent mettre en avant différents aspects de l'identité d'une personne qu'elle ne souhaite pas forcément lier à son identité officielle ou à d'autres identités numériques. De plus, les avantages potentiels d'une telle décision radicale pourraient ne pas compenser le préjudice causé à la liberté d'expression en ligne. En effet, il est important de noter que l'imposition de « vrais » noms sur les plateformes de réseaux sociaux n'a pas entraîné une diminution absolue du harcèlement. Des plateformes comme Facebook, qui appliquent cette politique, ne sont pas exemptes de harcèlement en ligne. Ainsi, bien que l'anonymat soit un facteur de désinhibition pouvant encourager les abus chez certains, le véritable moteur de ces comportements semble être le manque de responsabilité perçue, plutôt que la simple possibilité de rester anonyme.

6.3.2. Le mécanisme de pseudonymisation opposable

L'idée de mettre en place un système réglementaire et technique permettant l'utilisation de « pseudonymes opposables » est perçue comme une solution équilibrée. Elle permettrait de maintenir un niveau d'anonymat important pour les utilisateurs sur les réseaux sociaux, tout en offrant aux plateformes et aux autorités des outils pour mieux gérer la diffusion des discours haineux et des campagnes de désinformation en ligne.

Grâce à des techniques de cryptographie comme les preuves à divulgation nulle de connaissance (ZKP), les utilisateurs pourraient partager certains aspects de leur identité avec les réseaux sociaux sans donner à ces derniers un accès direct aux informations utilisées pour la vérification. Cela pourrait se faire par l'intermédiaire d'un tiers de confiance (comme une banque) ou d'un portefeuille numérique personnel, tel que celui développé par l'Union européenne (Commission européenne, 2023). Le service de vérification de confiance répondrait aux demandes des réseaux sociaux en confirmant un attribut, par exemple que la personne derrière la création du compte « est une personne » ou « à l'âge requis pour accéder au service », sans communiquer de nom, de numéro d'identification ou de date de naissance. Si ce système était développé en collaboration avec les gouvernements, il pourrait inclure une procédure permettant aux autorités compétentes de contourner le pseudonyme opposable et de le relier à l'identité d'une personne, facilitant ainsi les actions en justice contre les comportements illégaux sur les réseaux sociaux.

De plus, la possibilité de vérifier qu'un compte appartient à une personne physique créerait un nouveau niveau de contrôle pour les utilisateurs sur les réseaux sociaux. Ils pourraient, par exemple, paramétrer leurs préférences pour éviter tout contact avec des comptes non vérifiés et interagir uniquement avec des utilisateurs dont ils sont certains qu'il s'agit de personnes réelles. Cela pourrait limiter l'impact des réseaux de robots sur les interactions des utilisateurs sur les principales plateformes. Donner plus de contrôle aux utilisateurs des réseaux sociaux sur les personnes avec lesquelles ils acceptent d'interagir pourrait également réduire leur exposition aux abus et au harcèlement : d'une part en les protégeant des utilisateurs non vérifiés, et d'autre part en permettant l'identification de ceux qui, bien que vérifiés, adoptent des comportements illégaux.

Bien que cette approche préserve la possibilité pour les utilisateurs des réseaux sociaux de rester anonymes vis-à-vis des autres utilisateurs et des plateformes elles-mêmes s'ils le souhaitent, les gouvernements devraient aborder la mise en œuvre d'une telle solution avec prudence. La possibilité pour les autorités publiques de « casser » les identifiants numériques pourrait freiner l'adoption généralisée de cette mesure et potentiellement susciter l'opposition des minorités qui craignent que cela ne compromette leur capacité à s'exprimer à l'abri de toute surveillance ou répression extérieure. Cette crainte pourrait être atténuée en concevant le système ZKP de manière à ce que les tiers de confiance ne puissent pas savoir quelle plateforme de réseau social demande le jeton de vérification. Cela éliminerait la crainte des citoyens que le tiers de confiance possède une liste reliant l'identité réelle d'une personne et le jeton utilisé pour vérifier cette identité directement à la plateforme de réseau social

pour laquelle il a été généré, tout en maintenant la possibilité pour les autorités compétentes de créer ce lien si cela s'avère nécessaire dans le cadre d'une enquête justifiant cette intervention.

7. **Recommandations politiques et juridiques**

Reconnaissant le rôle de l'Union européenne dans l'élaboration des politiques numériques, le CEG identifie trois défis politiques critiques qui doivent être relevés. Pour relever ces défis, nous proposons une série de recommandations politiques qui visent à établir des systèmes d'identité numérique robustes, à garantir la protection de la vie privée grâce à l'anonymat et à renforcer l'application des réglementations existantes.

7.1. Percevoir l'anonymat dans un cadre que celui de la réglementation relative à la vie privée et à l'identité

Enjeu politique

Jusqu'à présent, le droit à l'anonymat en ligne n'a bénéficié que d'une reconnaissance limitée dans le cadre du droit et de la réglementation internationaux et ne peut être considéré comme un droit juridique universellement reconnu par les États. Toutefois, même si le droit international et la réglementation ont permis une reconnaissance limitée de ce droit, il est essentiel de reconnaître que lorsque les gouvernements et les acteurs privés surveillent les activités en ligne et recueillent des informations, ils violent les droits à la vie privée et à la protection des données. Ces violations diminuent la confiance des gens dans les services Internet et compromettent leur sécurité en ligne, ce qui a des conséquences négatives sur la libre circulation des idées et des informations sur Internet et porte atteinte à la liberté d'expression. Il est donc essentiel que les utilisateurs aient le droit à une correspondance privée, et il incombe à l'État de prendre toutes les mesures nécessaires pour garantir que les communications parviennent à leurs destinataires sans inspection ni ingérence de la part d'organes de l'État ou d'acteurs privés.

Recommandations politiques

Si le droit à l'anonymat en ligne, tout comme le droit à la liberté d'expression, ne peut être absolu, l'amélioration de la protection de la vie privée et des données en ligne peut contribuer à une société numérique plus démocratique qui respecte la liberté d'expression tout en évitant les risques de sécurité et de cybersécurité pour les États qui découlent d'un manque de responsabilité. Il est donc nécessaire que la Commission européenne adopte des lois efficaces sur la protection des données, qui définissent clairement qui est autorisé à accéder aux données personnelles des individus, à quelles fins ces données peuvent être utilisées, comment elles peuvent être stockées et pendant combien de temps.

Dans ce contexte, les réglementations existantes telles que le règlement général sur la protection des données (RGPD) ou le California Consumer Privacy Act of 2018

(CCPA) peuvent servir d'étalon-or transnational pour la protection des données, applicable à tous les transferts nationaux et transfrontaliers de données personnelles identifiables.

7.2. Orienter les solutions de vérification de l'identité numérique vers la réduction des abus en ligne, en consultation avec les parties prenantes

Enjeu politique

L'idée de rendre obligatoire la vérification de l'identité des utilisateurs des plateformes de réseaux sociaux refait régulièrement surface dans les débats concernant la possibilité pour les gouvernements de mettre en œuvre des solutions limitant la prolifération des abus en ligne, comme nous l'avons vu dans la section précédente. Cependant, la perspective de permettre aux entreprises de réseaux sociaux d'accéder directement aux attributs d'identité de tous les utilisateurs a toujours conduit les décideurs politiques à renoncer à une solution aussi radicale. L'avènement de projets visant à mettre en œuvre des identités numériques gouvernementales a néanmoins rendu possibles de nouvelles approches, telles que la mise en œuvre de protocoles ZKP. Ceux-ci pourraient combiner la préservation d'un niveau élevé d'anonymat pour les utilisateurs de réseaux sociaux avec des moyens d'action accrus pour les autorités, facilitant ainsi le recours légal contre les auteurs d'abus en ligne pour les victimes.
Il ne faut pas en déduire que tous les obstacles ont été levés, car nombre d'entre eux subsistent. L'un des défis liés aux tentatives de régulation de l'internet en général est que la législation nationale n'est que rarement applicable au-delà des frontières d'un pays, ce qui rend difficile le traitement des services en ligne opérant dans le monde entier. Cela reste vrai même pour les législations destinées à n'être appliquées qu'aux citoyens d'un seul pays, car l'utilisation répandue d'outils tels que les VPN permet aux utilisateurs de contourner facilement les obligations mises en œuvre pour leur pays.

Bien que l'UE ait l'habitude de projeter sa législation au-delà de ses frontières, il ne faut pas s'attendre à ce qu'il en soit de même pour la réglementation sur cette question, car les solutions proposées risquent de ne pas être suffisamment consensuelles ou réalistement applicables au niveau international.

La conception de protocoles de vérification d'identité qui ne font pas peser la charge de la vérification sur les plateformes de réseaux sociaux nécessitera d'assurer l'interopérabilité des systèmes entre plusieurs parties prenantes publiques et privées. L'interopérabilité peut avoir plusieurs définitions en fonction du contexte. Dans le cas de la réglementation européenne, nous pouvons distinguer deux approches principales, liées aux secteurs privé et public et toutes deux applicables dans le cadre réglementaire européen. La première est liée à la loi sur le marché numérique (DMA), qui introduit les concepts d'interopérabilité verticale et horizontale. L'interopérabilité verticale est limitée aux magasins d'applications et aux fonctionnalités essentielles des systèmes d'exploitation, tandis que l'interopérabilité horizontale s'applique aux fonctionnalités de base et aux gardiens fournissant des services de messagerie. En ce qui concerne le secteur public, l'un des principaux projets est *l'Interoperable Europe Act,* qui vise à créer un cadre transeuropéen pour l'infrastructure des services publics

numériques (Contrôleur européen de la protection des données, 2023). Enfin, l'identité numérique européenne est le projet le plus ambitieux, visant à créer un portefeuille numérique décentralisé permettant aux citoyens de l'UE de contrôler leurs données personnelles, conformément à la notion d'identité auto-souveraine (Commission européenne, 2023).

Recommandations politiques

À la lumière de ces défis, **à l'échelle internationale et européenne,** le CEG formule les recommandations suivantes afin d'orienter les discussions sur l'utilisation de solutions de vérification d'identité sécurisées qui protègent les données personnelles des utilisateurs :

⇒ **Engager des discussions au niveau international sur les stratégies de prévention des abus en ligne**. Les comportements illicites sur les plateformes de réseaux sociaux ne sont pas un problème propre à l'UE et ne peuvent être surmontés sans efforts concertés. C'est pourquoi l'UE doit s'efforcer de dégager un consensus international sur les meilleures pratiques susceptibles d'accroître la protection des utilisateurs sur les plateformes de réseaux sociaux en renforçant la responsabilité et les possibilités de recours juridique, sans compromettre la capacité des utilisateurs à opérer dans l'anonymat.

⇒ **Négocier un cadre pour les solutions de vérification d'identité en consultation avec les plateformes de réseaux sociaux.** Le cadre entourant les solutions de vérification d'identité devrait être élaboré par la Commission européenne en consultation avec les plateformes de réseaux sociaux. Toutefois, la protection des données personnelles des utilisateurs doit rester au centre de ces efforts, en créant un système qui ne permette ni à la plateforme de réseaux sociaux ni au tiers de confiance de créer des liens directs entre une identité réelle et un pseudonyme en ligne. Les protocoles « Zero Knowledge Proof » devraient donc être au cœur du débat.

⇒ **Permettre l'interopérabilité entre le projet européen d'identité numérique et les procédures de vérification d'identité mises en place**. Le **portefeuille numérique de l'UE** permettra aux utilisateurs/citoyens de stocker leurs données de manière décentralisée, ce qui leur permettra d'en garder le contrôle total. Il devrait être conçu pour être compatible avec les protocoles ZKP, ce qui permettrait de l'utiliser pour les procédures de vérification d'identité une fois qu'il sera officiellement lancé.

⇒ **Favoriser les échanges et l'innovation entre divers acteurs publics et privés.** Les citoyens devraient pouvoir choisir entre une variété de fournisseurs d'identité numérique et de tiers de confiance. Les entités privées et publiques devraient donc être encouragées à proposer des solutions d'identité numérique répondant aux besoins des utilisateurs et respectant les protections pertinentes accordées aux citoyens de l'UE par les règlements de l'UE.

Au niveau de l'État fédéral, le CEG formule les recommandations suivantes :

⇒ **Imposer la vérification d'identité uniquement lorsque cela est imposé par un objectif précis :** lutte contre les faux comptes, prévention des abus ou obligation de transparence pour certaines activités telles que les campagnes politiques en ligne.

⇒ **Inscrire toute vérification d'identité dans le cadre du RGPD** aux motifs de transparence sur le traitement des données, minimisation des données collectées, limitation de conservation, droit à l'effacement et absence de transfert hors UE sans garanties adéquates.

⇒ **Promouvoir l'adoption de solutions comme l'identité numérique auto-souveraine (Self-Sovereign Identity – SSI)** qui permettent aux utilisateurs de prouver certains attributs (âge, citoyenneté,...) sans révéler leur identité complète. Cela renforce la protection de la vie privée tout en assurant l'authenticité.

⇒ À l'instar de ce qu'il convient de réaliser au niveau européen, **introduire une législation nationale spécifique définissant le cadre d'utilisation des vérifications d'identité sur les plateformes sociales**, incluant les obligations de transparence pour les opérateurs et des mécanismes de contrôle par les autorités indépendantes comme l'Autorité de protection des données.

⇒ **Favoriser la coopération entre l'État, les acteurs privés et la société civile pour développer des solutions interopérables et standards ouverts.** Cela inclut l'intégration potentielle de systèmes d'identité numérique publique tels que **Itsme** dans les processus de vérification optionnelle ou volontaire.

7.3. Garantir la protection de la vie privée grâce à l'anonymat

Enjeu politique

L'objectif n'est pas de définir l'anonymat comme le droit d'être intraçable, mais plutôt de tirer parti de ses avantages, en accordant aux utilisateurs une meilleure protection des données. En d'autres termes, nous cherchons à conceptualiser l'**anonymat comme une garantie de respect de la vie privée** plutôt que comme un bouclier contre l'obligation de rendre des comptes.

Cette conception de l'anonymat soulève certaines questions politiques et juridiques, abordées dans nos recommandations. Au cœur de cette discussion se trouve le rôle central des plateformes de réseaux sociaux, qui non seulement facilitent l'anonymat mais agissent également comme des gardiens, en contrôlant l'accès aux informations des utilisateurs par des tiers et en gérant le traitement des données. Par conséquent, l'étendue de notre « droit à l'anonymat » dépend largement de ces plateformes. Il est donc impératif que l'Union européenne inscrive l'anonymat comme mesure de préservation de la vie privée dans la réglementation des plateformes. Il s'agit

d'appliquer et de faire respecter la protection des données personnelles par l'anonymat en établissant une passerelle entre le règlement général sur la protection des données (RGPD) et la loi sur les marchés numériques (DMA).

Un enjeu politique se présente donc : *comment la Commission européenne peut-elle garantir et renforcer le respect de la vie privée garanti par l'anonymat sur les réseaux sociaux par le biais du RGPD et de la DMA ?*

Recommandations politiques

Les dispositions relatives à l'**anonymisation des données à caractère personnel,** telles que l'article 6, paragraphe 11, de la loi sur la protection des données, posent deux grands problèmes :

⇒ *Comment trouver un équilibre entre une forte anonymisation et le maintien de la valeur des données ?*

⇒ *Comment relever le défi de l'anonymisation des données en conformité avec le* RGPD*, évitant ainsi toute réidentification possible ?*

Étant donné que l'anonymat et son application requièrent un niveau élevé d'expertise technique, ces recommandations combinent des mesures juridiques et techniques que le CEG conseille à l'UE d'adopter. Ainsi, la Commission pourrait :

⇒ **Améliorer et encourager l'adoption des technologies de renforcement de la protection de la vie privée.** Ces outils TIC minimisent la collecte, le traitement et le stockage des informations personnelles tout en permettant aux individus d'exercer un plus grand contrôle sur leurs données. Les technologies renforçant la protection de la vie privée suppriment ou transforment efficacement les informations personnelles identifiables, rendant la réidentification quasiment impossible.

⇒ **Établir des fiducies de données indépendantes afin de protéger la vie privée tout en facilitant l'accès aux données.** Les fonds de données collecteraient les données brutes des utilisateurs et les rendraient anonymes de manière appropriée, réduisant ainsi le risque de désanonymisation. En outre, les fonds de données pourraient fonctionner comme des bacs à sable, permettant à des algorithmes tiers d'analyser les données sans fournir d'accès direct aux données brutes. Toutefois, des défis pratiques liés à l'infrastructure, au coût et à la protection de la vie privée doivent être relevés, et la faisabilité d'une telle solution peut dépendre de la concentration sur des sous-ensembles spécifiques de données.

En outre, pour garantir l'efficacité du RGPD et de la DMA dans la réglementation et le contrôle de l'anonymat sur les réseaux sociaux, la Commission devrait :

⇒ **Assurer une interaction cohérente entre le DMA et le RGPD.** Il est essentiel de fournir une interprétation cohérente et de maintenir une **approche réglementaire harmonisée entre le DMA et le RGPD.** Plus précisément, étant donné que les dispositions de la DMA relatives à l'accumulation des données, aux interdictions d'utilisation croisée des données et aux obligations liées au partage des données sont étroitement liées au RGPD, l'UE doit garantir que la DMA ne porte pas atteinte aux principes énoncés dans le RGPD et qu'elle ne s'en écarte pas.

Au niveau de l'État fédéral, le CEG formule les recommandations suivantes :

⇒ **Élaborer un cadre légal national spécifique sur l'anonymisation** : définir des seuils, des méthodes reconnues et des responsabilités pour chaque type d'acteur (entreprises, chercheurs, institutions publiques).

⇒ **Créer une agence belge de l'anonymisation de données ou renforcer les compétences de l'Autorité de protection des données (APD)** en matière d'évaluation technique de l'anonymisation.

⇒ **Imposer des audits réguliers de ré-identifiabilité des données anonymisées utilisées par les plateformes de réseaux sociaux**, en coopération avec les autorités de contrôle européennes.

⇒ **Financer des projets pilotes dans le secteur public (santé, mobilité, emploi) pour tester des modèles d'anonymisation « privacy-preserving »,** tout en conservant la valeur statistique et analytique.

⇒ **Sensibiliser les citoyens et les développeurs** par l'intermédiaire de campagnes de communication et de formation portant sur l'enjeu de la ré-identification et des outils techniques de protection.

Bibliographie

I. Ouvrages académiques et scientifiques

A. De l'anonymat en ligne

- **Cardon, Dominique.** *À quoi rêvent les algorithmes : Nos vies à l'heure des big data*. Seuil, 2015.
- **Flichy, Patrice.** *Le sacre de l'amateur. Sociologie des passions ordinaires à l'ère numérique*. Seuil, 2010.
- **Morozov, Evgeny.** *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs, 2011.
- **Moyakine, Evgeni**. L'anonymat en ligne à l'ère numérique moderne : Quest for a Legal Right". *Journl of Information Rights Policy and Practice*, octobre 2016.
- **OCDE.** Technologies émergentes renforçant la protection de la vie privée. Approches réglementaires et politiques actuelles. *Documents de l'OCDE sur l'économie numérique, 2023.*

B. Sur la responsabilité en ligne et l'impunité

- **Citron, Danielle Keats.** *Hate Crimes in Cyberspace*. Harvard University Press, 2014.
- **Douillet, Anne-Laure.** *Internet et le droit : entre liberté et surveillance*. Presses Universitaires de France, 2018.
- **Persily, Nathaniel A.** Le défi d'Internet pour la démocratie : Définir le problème
et évaluer les réformes, 2019.

II. Articles scientifiques et juridiques

- **Bousquet, Françoise.** « L'anonymat sur Internet à l'épreuve du droit », *Revue Lamy Droit de l'immatériel*, 2013/97.
- **Cohen, Julie E.** « Configuring the Networked Self: Law, Code, and the Play of Everyday Practice », *Yale Journal of Law & Technology*, 2012.

- **Rouvroy, Antoinette & Berns, Thomas.** « Le nouveau pouvoir statistique », *Multitudes*, 2013.
- **Demircan, Muhammed.** Le DMA et le GDPR : Comprendre les dispositions relatives à l'accumulation, à l'utilisation croisée et au partage des données, 2022.
- **Demircan, Muhammed.** Le DMA et le GDPR : Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions". *Vrije Universiteit Brussel*, décembre 2022.

III. Articles de presse et sources médiatiques (grand public)

- **Le Monde** :

  « L'anonymat en ligne de plus en plus remis en cause par les gouvernements» – Le Monde, 2022
- **France Inter** :

  « Peut-on encore rester anonyme sur les réseaux sociaux ? » (Podcast, 2021)
- **The Guardian** :

  "Should Anonymity on Social Media Be Banned?" – *The Guardian*, 2021

IV. Sources législatives et réglementaires

- **RGPD (Règlement général sur la protection des données)** – UE, 2018
- **Digital Services Act (DSA)** – Union Européenne, 2022

V. Études de cas et rapports d'organisations

- **Reporters sans frontières (RSF)** :

  Classement mondial de la liberté de la presse – éditions 2022-2024
- **Human Rights Watch** :

  Protecting Anonymity Online (2020)
- **Commission européenne** :

  Study on the use of anonymous accounts and its link to illegal online content, 2021

VI. Outils et aspects techniques

- **Chaum, David.** « Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms », *Communications of the ACM*, 1981.
- **EFF (Electronic Frontier Foundation)** :
  Ressources sur *Tor*, *VPN*, et autres outils d'anonymisation :
  https://www.eff.org