SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Faut-il mettre fin à l'anonymat sur les réseaux sociaux ?

Lorenzo Ancona, Gabriel Karl,

Arnau Martì & Wiktor Samek

Approche comparative de la réglementation des grandes technologies (printemps 2023)

Professeur Florence G'sell

Avril 2023

Table des matières

Résumé

À l'époque contemporaine, l'anonymat peut sembler anachronique. Les solutions techniques actuelles nous ont considérablement exposés à la surveillance par des acteurs privés et publics. En outre, notre identité numérique est devenue une marchandise livrée et utilisée par les grandes entreprises technologiques. Parallèlement, les questions relatives à la désinformation et à la vérification des utilisateurs peuvent donner l'impression que l'anonymat est potentiellement dangereux pour notre société et notre démocratie. Les plateformes de réseaux sociaux sont un excellent exemple de ces phénomènes, soulignant à quel point il est crucial de protéger notre vie privée et notre identité.

Dans notre article, nous démontrons que l'anonymat reste un outil valable pour protéger notre vie privée sur les réseaux sociaux. Nous reconnaissons les limites inhérentes à l'anonymat, mais au lieu de les utiliser comme une raison de rejeter complètement le concept, nous nous efforçons de les adapter de manière créative pour construire de meilleurs modèles de régulation. Par conséquent, en nous appuyant sur la nature contextuelle et pseudonyme de l'anonymat numérique moderne, nous proposons une solution innovante qui fusionne l'anonymat avec l'exigence de vérification et un niveau adéquat de confidentialité et de contrôle des données des utilisateurs par eux-mêmes. Nos recommandations s'appuient sur la recherche universitaire et les cadres juridiques, avec un accent particulier sur la Commission européenne, qui est la cible de nos préconisations.

D'une manière générale, nous invitons les institutions européennes à percevoir l'anonymat comme une opportunité de créer un environnement plus respectueux de la vie privée sur les réseaux sociaux. Pour garantir le respect des dispositions de la loi sur le marché numérique (DMA) et du règlement général sur la protection des données (GDPR), l'UE devrait renforcer l'adoption de technologies améliorant la protection de la vie privée et établir des fiducies de données autonomes. L'UE doit également assurer une interaction et une interprétation cohérentes entre la loi sur le marché numérique et le règlement général sur la protection des données. Nous encourageons les institutions européennes à étudier les solutions d'identité numérique en tant qu'approche potentielle pour résoudre les problèmes de vérification, tout en préservant la vie privée et l'anonymat. Nous pensons que des solutions publiques telles que l'identité numérique européenne peuvent être appliquées dans ce domaine, mais pas en tant que moyen obligatoire d'autorisation de l'utilisateur. Nous recommandons plutôt de développer une politique d'interopérabilité avec les acteurs privés qui offre aux citoyens de l'UE une gamme

d'options adaptées à leurs besoins spécifiques. Toutes ces mesures renforceront considérablement la position des citoyens ordinaires vis-à-vis des plateformes de médias sociaux, sans placer trop d'informations privées précieuses sous le contrôle d'une autre autorité centrale, en utilisant l'anonymat d'une manière moderne et responsable.

Introduction

L'anonymat est-il un droit fondamental sur Internet ? Devrions-nous pouvoir dissimuler notre véritable identité sur les plateformes de médias sociaux tout en continuant à les utiliser ? Comment trouver un équilibre entre le droit à l'anonymat et la nécessité de rendre des comptes ? À l'inverse, l'anonymat est-il essentiel pour préserver notre vie privée lorsque nous naviguons dans le monde numérique ? Notre mémoire a été inspiré par ces questions stimulantes sur l'anonymat et ses implications à l'ère numérique. Pour y répondre, nous avons tenté de disséquer la notion complexe d'anonymat sur les réseaux sociaux, en évaluant ses avantages et ses risques et en fournissant une vue d'ensemble des différentes approches réglementaires et politiques. Sur cette base, nous avons élaboré des recommandations politiques ciblées pour aborder la question intrigante de l'anonymat.

Dans la première section, nous cherchons à **définir l'anonymat** et à mettre en évidence son lien critique avec la vie privée. En analysant le fonctionnement interne et la dynamique des réseaux sociaux, nous constatons que l'anonymat est un concept contextuel et relationnel, ce qui rend l'anonymat complet impossible à atteindre sur les médias sociaux. En outre, en nous appuyant sur le concept de "vie privée informationnelle" de Floridi, nous reconnaissons l'**interdépendance entre l'anonymat et la vie privée**, le premier étant une condition préalable à la seconde.

Dans la deuxième section, nous présentons une analyse complète de l'anonymat, en détaillant à la fois ses **avantages** et ses **risques** afin d'apporter une compréhension globale. Les avantages englobent la liberté d'expression, la protection de la vie privée

et la divulgation de soi, tandis que les risques comprennent la cyberintimidation, la désinformation et les activités illégales.

Notre analyse est complétée dans la troisième section par l'examen des **approches politiques et juridiques de l'anonymat.** Nous comparons les systèmes juridiques qui protègent l'anonymat, comme ceux des États-Unis, de l'Union européenne et du Royaume-Uni, avec ceux qui adoptent une approche plus restrictive. En outre, d'un point de vue politique, nous mettons en lumière diverses politiques conçues par les régulateurs pour traiter de l'anonymat et de ses implications.

Enfin, sur la base de notre analyse complète, nous ciblons l'Union européenne et identifions trois défis politiques critiques, auxquels nous répondons par **trois recommandations politiques**. Nous abordons la nécessité de systèmes d'identité numérique, l'application des réglementations et la protection de la vie privée grâce à l'anonymat.

1. Le concept d'anonymat : une vue d'ensemble

L'anonymat est naturellement lié au cyberespace. À bien des égards, il s'agissait d'une grande promesse du web au moment de sa création. Mais c'était aussi un acte de capitulation. Dans sa célèbre *Déclaration d'indépendance du cyberespace,* J. P. Bartlow écrivait : "Nos identités n'ont pas de corps : *Nos identités n'ont pas de corps, donc, contrairement à vous, nous ne pouvons pas obtenir l'ordre par la coercition physique* (Barlow, 1996). De nombreux cyber-enthousiastes ont observé à juste titre les changements provoqués par l'internet en ce qui concerne nos identités. Cependant, Barlow et d'autres ont commis une grave erreur en supposant que cette identité serait hors de portée des pouvoirs traditionnels du monde matériel. De plus, il est rapidement devenu clair que cette nouvelle identité est en fait délivrée par des acteurs émergeant des changements de la révolution du Web 2.0, à savoir les plateformes de réseaux sociaux. L'anonymat peut être perçu comme une réponse à cette question[1].

[1] Elle est devenue le symbole du collectif Anonymous fondé en 2003 pour s'opposer à la limitation de la "liberté primitive" sur Internet (Cadwalladr, 2012).

Dans cette partie du texte, nous allons aborder ces questions. Tout d'abord, nous présentons notre propre définition de l'anonymat. Ensuite, nous montrons son lien avec les notions de vie privée et d'identité. Nous montrerons clairement les deux changements provoqués par l'essor des plateformes de médias sociaux, qui sont cruciaux pour notre analyse et nos recommandations présentées dans les parties suivantes du document.

1.1 Jusqu'à quel point pouvons-nous être anonymes ? Une définition de l'anonymat

Donner une définition claire de l'anonymat n'est paradoxalement pas très difficile. Cependant, ce qui est vraiment important, c'est de comprendre qu'il s'agit d'une notion très différente de l'acception populaire de ce terme. Nous avons tendance à percevoir l'anonymat comme un état excluant toute possibilité d'identification. En réalité, l'anonymat est toujours contextuel ou relationnel (Wallace, 1999, pp. 23-24). Il n'est donc 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. Cependant, il partage des idées ou des compétences, ces deux éléments faisant partie de son identité.[2] En outre, un auteur peut construire son capital artistique sur la base de publications anonymes ou pseudonymes (Scott et Orlikowski, 2014, p. 876). Il s'agit là d'une **limitation ontologique** profonde de l'anonymat.

En outre, il y a une question de savoir-vivre. Existe-t-il un moyen vraiment efficace de parvenir à l'anonymat, même sous cette forme limitée ? Pour revenir à l'exemple de l'"auteur anonyme", nous pouvons utiliser les fragments connus de l'identité pour en décoder les autres éléments. En outre, plus une personne écrit de livres, plus il est facile de révéler l'ensemble du tableau. C'est d'autant plus important que dans la réalité des médias sociaux, nous devons nous débarrasser de centaines de messages et d'autres activités qui, dans certains cas, peuvent être aussi importants pour révéler l'activité d'une personne. Si l'on ajoute les méthodes sophistiquées

[2] Comme nous l'expliquerons dans la partie suivante, nous acceptons, pour les besoins de notre texte, la définition moderne et large de l'identité.

d'acquisition et d'analyse des données dont disposent les entreprises de médias sociaux, il est justifié d'affirmer que l'anonymat total est pratiquement impossible dans la réalité des plateformes de médias sociaux (Scott et Orlikowski, 2014, p. 877).

Le caractère de plateforme des médias sociaux est essentiel pour comprendre les limites de l'anonymat qu'ils autorisent. En effet, la plateforme ne nous "permet" pas vraiment d'être anonymes, elle nous fournit l'anonymat. Par conséquent, l'anonymat n'est en quelque sorte qu'une autre fonctionnalité de la plateforme. Cela est lié au concept de *dissociabilité. L'anonymat* peut être analysé du point de vue de l'*expéditeur* et du *destinataire* ou de la *relation.* Les deux premiers nous indiquent si nous pouvons relier un message particulier à l'utilisateur qui l'a envoyé ou reçu. L'*anonymat relationnel* est lié à la possibilité d'observer l'échange d'informations entre des utilisateurs spécifiques (Pfitzmann *et al.*, 2007, p. 9). Une plateforme de médias sociaux peut facilement retracer ces connexions car elles font toutes partie d'un processus qui se déroule presque exclusivement sur l'infrastructure de la plateforme. Sans contraintes internes ou externes, la plateforme peut suivre le processus depuis le moment où les données sont téléchargées via son application, en passant par le traitement qui a lieu sur ses serveurs, jusqu'au moment où elles sont finalement reçues, également via son logiciel, du côté du destinataire.

Dans le même temps, le **caractère contextuel de l'anonymat** se traduit par l'importance de la taille de la population (Pfitzmann *et al.*, 2007). Dans ce contexte, les plateformes de médias sociaux sont paradoxales. Elles rassemblent un nombre massif d'utilisateurs, mais les relations entre eux sont en quelque sorte similaires à celles qui caractérisent les très petites communautés. L. Floridi a illustré cela par une comparaison intéressante entre le village *local* et le village *global* et leur relation avec le concept de vie privée. Dans les deux cas, nous avons affaire à des communautés ouvertes. L'échange d'informations est public et la distance entre les individus est courte, limitée par les conditions matérielles ou les outils technologiques. Les différences sont toutefois cruciales, car le *village planétaire* ne protège pas ses membres grâce à un réseau dense d'autorégulation informelle et formelle (Floridi, 2014, p. 112). Nous pouvons donc conclure que les plateformes de médias sociaux

créent un environnement qui expose notre vie privée à une échelle sans précédent, à la fois par rapport aux autres utilisateurs et à la plateforme elle-même. L'anonymat, tel qu'il est perçu dans le contexte, peut en quelque sorte protéger notre vie privée des autres utilisateurs, mais pas de l'ingérence de la plateforme ou des gouvernements. Dans ce dernier cas, les régimes autoritaires sont déjà très efficaces pour limiter les possibilités d'atteindre un anonymat en ligne, même limité (Bode et Makarychev, 2013). Dans le même temps, les pays démocratiques deviennent de plus en plus efficaces pour traquer les cybercrimes ou même intercepter les communications cryptées entre les criminels (EUROJUST, 2023), sans parler des utilisateurs réguliers de l'internet qu'il est possible de traquer par des méthodes moins sophistiquées telles que l'utilisation de leur numéro IP.

En outre, la méta-analyse des données se situe actuellement à un niveau tel qu'il est difficile de parler d'anonymat, même sur des plateformes véritablement décentralisées (De Filippi, 2016). L'infrastructure basée sur la blockchain en est un parfait exemple. Grâce à une cryptographie avancée, les utilisateurs des plateformes sociales basées sur la blockchain sont en mesure de dissimuler leur personnalité derrière des pseudonymes. Néanmoins, la fonctionnalité clé des réseaux blockchain est également la transparence, car toutes les interactions sont stockées dans le grand livre ouvert. Par conséquent, son analyse peut, de manière relativement efficace, découvrir des éléments particuliers de l'identité d'une personne et finalement permettre son identification correcte. Dans notre analyse et nos recommandations, nous nous concentrons sur les grandes plateformes de médias sociaux centralisées, mais il est important de noter que même leurs concurrents décentralisés n'introduisent pas la nouvelle version parfaite de l'anonymat.

Sur la base de ce qui précède, nous pouvons donner une définition de l'anonymat qui sera utilisée dans notre document :

1. Nous acceptons la définition classique de l'anonymat comme ***un état où l'on ne peut pas être identifié au sein d'un ensemble de sujets*** (Pfitzmann *et al.*, 2007, p. 6).

2. En même temps, nous reconnaissons le **caractère contextuel et relationnel de l'anonymat** qui rend impossible la possibilité d'anonymat au sein de tous les ensembles de sujets et par rapport à toutes les parties du processus de communication.
3. Nous pensons que les possibilités d'**anonymat sur les médias sociaux sont massivement limitées**, pour les raisons suivantes
    a. les possibilités offertes par la méta-analyse des données,
    b. une forte dépendance à l'égard des plateformes de médias sociaux en ce qui concerne notre identité numérique et notre vie privée,
    c. les capacités croissantes de l'État à surveiller toutes les activités qui se déroulent en ligne.
4. C'est pourquoi les plateformes centralisées et décentralisées proposent le pseudonymat plutôt que l'anonymat, ce qui permet aux utilisateurs d'utiliser des pseudonymes au lieu de leur vrai nom (ibidem, p.14), mais pas de rester réellement non identifiables. Néanmoins, par souci de clarté, nous utiliserons dans la suite du texte le terme "anonymat" plutôt que "pseudonymat", en gardant à l'esprit toutes les remarques susmentionnées.

Tant dans la définition présentée que dans la partie précédente du texte, nous avons mentionné les notions de vie privée et d'identité. Comme il s'agit des phénomènes protégés par l'anonymat, nous examinerons dans les prochaines parties comment ils ont évolué dans l'environnement des médias sociaux et comment cela a modifié notre perception de l'anonymat.

1.2 À qui appartient réellement notre identité ?

L'identité numérique peut être comprise de deux manières : comme une **solution technique** permettant l'identification d'une personne dans le cyberespace ou comme un **ensemble spécifique de données** traduisant l'identité sociale d'une personne sur le web (Feher, 2021, p. 193).

En ce qui concerne ce dernier point, notre définition de l'anonymat repose sur une conception large de l'identité, conforme à la psychologie moderne, qui la définit

comme *une configuration intégrative de soi dans le monde adulte* (McAdams, 2001, p. 102). Par conséquent, dans le contexte des médias sociaux, l'identité ne signifie pas simplement le nom d'une personne. Au contraire, notre identité numérique évolue dans le sens d'une moindre connexion avec elle. C'est pourquoi des auteurs comme L. Floridi affirment que notre décision concernant notre identité dans le cyberespace n'est plus vraiment liée au choix entre l'anonymat et l'ouverture. Cela est devenu impossible dans le monde de la surveillance quasi constante exercée sous des formes plus ou moins ouvertes par les gouvernements et les entreprises privées. Ce qui reste, c'est la capacité de décider de la forme de l'identité imaginaire que nous voulons créer sur la plateforme sociale (Floridi, 2014, p. 64). Toutefois, notre pouvoir en la matière est également limité par le caractère relationnel de l'identité. Les plateformes sociales ont créé une notion de *regard numérique* (Floridi, 2014, p. 73). Cela signifie que les utilisateurs de la plateforme se perçoivent presque exclusivement à travers la perception des autres utilisateurs. Par conséquent, une personne particulière est réduite à la production du processus d'établissement de l'identité, qui se déroule en grande partie hors de sa portée. Dans ce contexte, le contrôle que les plateformes exercent sur les algorithmes et leurs politiques de promotion des contenus leur confère un contrôle sur la création de notre identité, en particulier dans le cas des utilisateurs les plus jeunes. Cela a des conséquences majeures pour l'anonymat, car cacher une partie de notre identité en ligne n'a aucun sens, tant qu'elle est développée dans le cadre d'un processus non contrôlé par l'utilisateur.

La question de l'identité numérique d'un point de vue technologique est analysée principalement dans le contexte du fournisseur éventuel de cette solution et de son caractère public ou privé. Les solutions fournies par le gouvernement sont actuellement utilisées dans l'administration publique, mais des acteurs tels que la Commission européenne prévoient d'étendre leur utilisation à d'autres secteurs (Commission européenne, 2021) et des solutions décentralisées basées sur la blockchain sont mises en œuvre à titre expérimental pour garantir aux personnes un meilleur contrôle de leur identité (Mühle *et al.*, 2018). Néanmoins, dans la réalité des médias sociaux, l'identité numérique est toujours fournie principalement par la plateforme. Par conséquent, être anonyme sur le web devient de plus en plus problématique en raison du

développement de moyens d'identification plus efficaces dans le cyberespace par le gouvernement, ainsi que de la dépendance à l'égard des solutions privées, souvent renforcée par la connexion de différents services à une seule identité numérique.

1.3 Comment assurer la protection de la vie privée en public ?

L'anonymat est tellement lié à la vie privée que, pour beaucoup, ces deux notions sont synonymes. Néanmoins, en ce qui concerne le contenu des médias sociaux, nous devons tout d'abord nous concentrer sur les données, puis reconnaître les différences significatives dans la perception de la vie privée dans les différentes cultures juridiques[3] . Pour simplifier, nous pouvons dire que l'Europe continentale a développé le concept de vie privée comme un moyen de défendre sa dignité, alors que la culture américaine est plus orientée vers la notion de liberté (Whitman, 2004). Les Européens sont donc plus préoccupés par les questions du *droit à l'autodétermination informationnelle* (ibidem, p. 1161) et de la protection de la dignité de l'individu dans ses rapports avec les acteurs privés, tandis que les Américains ont tendance à cultiver une approche plus ancienne, en essayant de limiter l'ingérence de l'État dans la vie de l'individu (ibidem). Nous avons démontré plus haut que l'État et les entreprises privées peuvent limiter l'anonymat sur les médias sociaux. Il est naturel que des cultures juridiques différentes perçoivent et réglementent ces questions différemment.

Pour ce qui est de la compréhension de la **confidentialité des informations**, nous avons adapté dans notre travail le cadre créé par L. Floridi. Il a déclaré que la *confidentialité des informations est une fonction de la friction ontologique dans l'infosphère* (Floridi, 2005, p. 187), où la *friction ontologique* représente les forces qui s'opposent au flux d'informations (ibidem, p. 186). La valeur de cette approche du point de vue de l'élaboration des politiques est évidente. Tout d'abord, Floridi a remarqué le changement ontologique qui se produit avec les plateformes de médias sociaux et l'internet en général. Les nouveaux moyens technologiques ne modifient pas l'infosphère, ils créent un modèle complètement nouveau au niveau ontologique. Deuxièmement, cela signifie que nous ne pouvons pas porter de jugements généraux

[3] Dans le cadre de ce document, il s'agit bien entendu des différentes cultures juridiques occidentales, c'est-à-dire l'Europe continentale et les États-Unis.

sur la vie privée dans le cyberespace, nous devons analyser des éléments particuliers de la nouvelle infosphère. Troisièmement, même les changements technologiques précédents n'étaient pas synonymes de limitation inconditionnelle de notre vie privée. Il en va de même pour l'internet, qui a à la fois créé un dépôt plus ou moins ouvert de nos informations privées et nous a offert des possibilités sans précédent en matière d'anonymat ou de cryptage des informations.

Par conséquent, en ce qui concerne la vie privée, nous reconnaissons son lien avec l'anonymat. Il est important de rappeler que, tant dans le cas d'acteurs gouvernementaux que privés, les médias sociaux ne peuvent garantir le respect de la vie privée sans un certain niveau d'anonymat, puisque, par définition, le respect de la vie privée implique que certaines parties de nos données personnelles (identifiées) restent hors de leur portée.

1. 2. Avantages et risques de l'anonymat sur les médias sociaux

À l'ère de l'information (voir Floridi, 2010), l'anonymat englobe une interaction complexe entre différents domaines, notamment la vie privée, la responsabilité et la liberté d'expression dans les régimes démocratiques et non démocratiques. Par conséquent, un examen approfondi des avantages et des risques de l'anonymat permet de bien comprendre ses implications et d'élaborer des recommandations politiques efficaces.

2.1 Avantages et opportunités

2.1.1 Liberté d'expression

L'anonymat peut contribuer de manière significative à la liberté d'expression en favorisant des **discussions ouvertes sur des sujets sensibles** et en offrant **un refuge sûr aux voix dissidentes**, en particulier dans des environnements politiquement oppressifs.

Tout d'abord, les individus sont plus susceptibles d'exprimer leurs opinions et leurs pensées sur les médias sociaux sans craindre de répercussions politiques ou

personnelles (Nissembaum, 1999). Ils peuvent notamment oser prendre des positions ou participer à des discussions qu'ils n'auraient pas engagées autrement. Par conséquent, l'anonymat conduit à un **discours public plus diversifié et plus ouvert**, ce qui profite aux sociétés démocratiques. (Nissembaum, 2009)

Deuxièmement, comme la numérisation alimente la croissance des organisations de **lanceurs d'alerte** et de **militants** et que les médias sociaux sont essentiels pour diffuser les fuites d'informations, l'anonymat est crucial pour protéger ces personnes contre d'éventuelles représailles ou préjudices (Olesen, 2019). Le printemps arabe en est un bon exemple : les militants se sont appuyés sur des comptes anonymes de médias sociaux pour organiser des manifestations et partager des informations sur les mesures de répression du gouvernement tout en évitant d'être repérés par les autorités de l'État (Howard et al., 2011).

2.1.2 Protection de la vie privée

À une époque où l'on s'inquiète de plus en plus de la collecte de données personnelles (Zuboff, 2015) et où l'on reformule le concept même de vie privée (Floridi, 2014), l'anonymat peut offrir aux utilisateurs des avantages considérables en matière de protection de la vie privée. Comme le note Floridi (2005), la "vie privée informationnelle" n'est pas seulement le contrôle des données personnelles, mais aussi la tentative de conserver son identité et son autonomie.

Les comptes anonymes des médias sociaux et les interactions en ligne peuvent **protéger les utilisateurs d'un examen indésirable** et leur permettre de limiter la circulation de leurs informations personnelles. Toutefois, comme le précise la section 1 [Le concept d'anonymat], il n'est pas possible de parvenir à un véritable anonymat et à une protection totale contre l'identification par les médias sociaux. Néanmoins, en adoptant cette notion de traçabilité partielle, les utilisateurs peuvent éviter de laisser derrière eux des traces de données personnelles exploitables à des **fins commerciales ou malveillantes**, telles que l'usurpation d'identité (Nissembaum, 2004).

En outre, l'anonymat trace une ligne de séparation 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

permet aux individus de reprendre le contrôle des données qu'ils préfèrent ne pas partager en ligne et réduit le risque d'un suivi malveillant qui pourrait relier leurs activités à leurs identités.

2.1.3 Divulgation de soi et santé mentale

Bien que le champ d'application soit restreint par rapport à la liberté d'expression et à la protection de la vie privée, l'anonymat sur les médias sociaux s'est avéré important pour les personnes cherchant un soutien pour des questions sensibles et potentiellement stigmatisantes, telles que les problèmes de santé mentale, les addictions ou les traumatismes.

L'anonymat facilitant la **divulgation de soi et la désinhibition en ligne** (Suler, 2004), les utilisateurs peuvent exprimer leurs sentiments, demander conseil et partager leurs expériences sans craindre d'être jugés ou de subir des conséquences sociales négatives (Lawlor et Kirakowski, 2014). Des études ont montré que cela avait un impact positif sur le bien-être psychologique (Frye et Dornisch, 2010).

2.2 Risques et défis

L'anonymat sur les médias 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.** En tant que problème critique résultant de l'anonymat, la responsabilité sera examinée et discutée en détail dans les sections suivantes de cette note d'information.

2.2.1 Cyberintimidation et harcèlement.

L'utilisation généralisée des médias sociaux combinée à l'anonymat a favorisé les interactions entre les utilisateurs, y compris des pratiques telles que le **harcèlement en ligne** et la **cyberintimidation**. L'anonymat est propice à la cyberintimidation (Whittaker et Kowalski, 2015), car l'absence d'informations identifiables permet aux utilisateurs de se livrer à des comportements préjudiciables avec peu ou pas de conséquences, puisqu'il devient difficile de remonter jusqu'à l'auteur de ces actions (Aboujaoude et al., 2015). Cette absence de responsabilité peut favoriser un environnement en ligne toxique, où les utilisateurs se sentent encouragés à adopter

des comportements agressifs ou abusifs qu'ils ne manifesteraient pas dans des interactions en face à face.

Par conséquent, le degré et la fréquence élevés de la cyberintimidation peuvent entraîner une grave détresse psychologique chez les victimes, qui souffrent d'anxiété, de dépression, d'une faible estime de soi, voire d'idées suicidaires (Patchin et Hinduja, 2010).

2.2.2 Désinformation

La prolifération des fausses nouvelles et de la propagande mensongère est un défi important posé par l'anonymat sur les médias sociaux. L'anonymat est un terrain fertile pour les **robots**, les **faux comptes** et les **conversations inauthentiques** sur divers sujets, ce qui conduit à un écosystème d'information en ligne peu fiable et peu digne de confiance qui peut avoir des conséquences dans le monde réel.

Les robots des médias sociaux, définis comme des "comptes automatisés capables de produire du contenu et d'interagir avec des utilisateurs humains sur les plateformes de médias sociaux" (Ferrara et al., 2016), prospèrent dans un environnement qui privilégie l'anonymat en ligne (Persily, 2019). La plupart des gens accédant aux informations par le biais des médias sociaux (Gottfried et Shearer, 2016), les bots jouent un rôle décisif dans l'orientation du débat public en diffusant des fausses nouvelles en ligne sur des sujets allant de la politique à la santé. Les bots sont programmés pour amplifier des récits spécifiques ou influencer l'opinion publique, manipulant ainsi les médias sociaux et trompant les utilisateurs pendant les phases initiales, avant que le contenu n'atteigne un statut viral, et ils se concentrent sur l'engagement avec les utilisateurs influents par le biais de réponses et de mentions. Cette susceptibilité à la manipulation est évidente car les individus ont tendance à retweeter les bots partageant des contenus peu crédibles presque aussi souvent qu'ils retweetent d'autres personnes (Shao et al., 2018). Persily (2019) décrit cela comme un **"engagement non responsable"**, où il n'est pas clair non seulement *qui* parle, mais aussi *si* le discours provient d'une personne réelle. Enfin, l'anonymat offert par les plateformes de médias sociaux fait qu'il est difficile de retracer les origines des créateurs de robots ou de les tenir pour responsables de la diffusion de fausses informations (Ferrara, 2020).

Cet environnement de désinformation en ligne entraîne un large éventail de **conséquences dans le monde physique**, allant de la manipulation pendant les campagnes électorales (Allcott et Gentzkow, 2017) à la diffusion de fausses informations liées à des questions de santé publique (Shahi et al., 2021).

2.2.3 Activités illégales

L'anonymat sur les plateformes de médias sociaux peut servir de refuge à des individus et à des groupes pour participer à toute une série d'activités illégales. Par exemple, les utilisateurs anonymes peuvent partager des **contenus illicites**, tels que de la pornographie enfantine ou des documents protégés par des droits d'auteur, en se cachant derrière l'anonymat en ligne sans craindre d'être identifiés et, par conséquent, poursuivis en justice. (UNICEF, 2022). En outre, l'anonymat incite les pirates informatiques et les cybercriminels à mener d'autres activités criminelles telles que l'**usurpation d'identité, l'hameçonnage ou le lancement de cyberattaques**, avec un risque réduit d'être tracés (Sullins, 2006).

Les technologies de communication numérique et l'anonymat influencent également de manière significative la **radicalisation** et le **recrutement** (Meleagrou-Hitchens et al., 2017). Cet environnement permet aux groupes extrémistes de diffuser leur propagande et de recruter des adeptes potentiels, favorisant ainsi la radicalisation dans certains contextes. En particulier, des individus insoupçonnés qui ne s'engageraient pas dans de telles activités hors ligne profitent de l'environnement anonyme offert par l'internet (McFarlane, 2010). En effet, comme l'a constaté Koehler (2014), l'anonymat est un facteur clé qui pousse les individus à adopter des points de vue et des groupes extrémistes.

2. 3. Approches politiques et juridiques

Nous poursuivons notre analyse du concept d'anonymat en examinant divers systèmes réglementaires et approches politiques. Dans la première partie de cette section, nous examinons la manière dont les régulateurs ont appliqué les règles relatives à l'anonymat, en étudiant les systèmes libéraux et les régimes autoritaires. Puis, dans la

deuxième partie, nous décrivons certaines politiques conçues pour faire face à l'anonymat et à ses implications.

3.1. Réglementations existantes sur l'anonymat

Dans cette section, nous observerons comment les réglementations existantes appliquent l'anonymat en ligne dans différents pays. Bien que chaque pays ait une jurisprudence différente, nous avons identifié deux positions distinctes : les pays qui reconnaissent l'anonymat comme un droit légal et ceux qui appliquent une approche restrictive.

Nous explorerons donc les nuances de l'anonymat en ligne en tant que droit légal dans différentes régions, notamment en Amérique du Nord, au Royaume-Uni et dans l'Union européenne, ainsi que l'approche restrictive contrastée de l'anonymat en ligne dans les pays où la liberté des médias est limitée, tels que la Russie et la Chine.

3.1.1 L'anonymat en ligne : un droit

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. Toutefois, garantir l'anonymat est complexe, car 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 (Moyakine, 2016).

A. États-Unis et Amérique du Nord

Aux États-Unis, la Cour suprême protège traditionnellement les discours anonymes en vertu du premier amendement, mais, comme pour d'autres droits constitutionnels, elle met en balance cette protection avec des intérêts concurrents, notamment dans les domaines de l'activité politique et du financement des campagnes

électorales, par exemple. Sur l'internet, la Cour suprême a reconnu le droit à l'anonymat dans les discours, mais pas comme un droit absolu, et les tribunaux des États ont généralement adopté un point de vue similaire.

Dans "The United States of Anonymous : How the First Amendment Shaped Online", l'auteur Jeff Kosseff explore deux affaires, *Dentrite International, Inc. v. Doe* No. 3, 775 A.2d 756 (N.J. App. Div. 2001) et *Cahill v. Doe*, 879 A.2d 943 (Del. Super. Ct, 14 juin 2005), dans lesquelles les tribunaux ont reconnu des présomptions relativement fortes du premier amendement en faveur des fournisseurs de discours anonymes, en particulier pour ceux qui sont des déclarations d'opinions plutôt que des mensonges évidents, tout en reconnaissant que le gouvernement a parfois le droit d'identifier ces orateurs lorsqu'ils ont utilisé leurs plateformes pour harceler, se livrer à la calomnie ou à la prédation sexuelle, proférer de véritables menaces ou permettre à des gouvernements étrangers d'influer sur les élections américaines. (Martin et Fargo, 2015)

En droit canadien, ce droit est parfois reconnu comme étant lié au droit à la vie privée. En ce qui concerne l'anonymat en ligne, les tribunaux canadiens ont mis au point un test d'équilibre exigeant que la partie cherchant à obtenir l'identification d'utilisateurs anonymes démontre d'abord qu'elle a une demande de *bonne foi* et qu'il n'y a pas d'autre source d'information nécessaire. Si la partie peut faire cette démonstration, le tribunal doit peser les facteurs favorables ou défavorables à la divulgation. Les tribunaux canadiens ont élaboré ce test dans une affaire concernant une tentative de démasquer les clients d'un fournisseur d'accès à Internet qui auraient violé les droits d'auteur du plaignant (Martin et Fargo, 2015).

B. ROYAUME-UNI

De même, en 1973, la Chambre des Lords a établi un test concernant les conditions dans lesquelles un plaideur peut obliger un tiers à identifier des défendeurs potentiels dans le cadre d'un procès. La partie qui demande l'information doit démontrer que (1) la partie inconnue a vraisemblablement commis une faute à l'encontre du plaignant ; (2) l'identification de la partie inconnue est nécessaire ; et (3) le tiers est en mesure d'identifier l'auteur présumé de la faute. Les tribunaux sont censés mettre en

balance les intérêts du tiers à préserver la confidentialité et les intérêts de la justice. Ce critère a également été utilisé dans d'autres procès au Royaume-Uni concernant des tableaux d'affichage sur Internet et d'autres publications en ligne (Martin et Fargo, 2015).

C. L'Union européenne

Le droit européen tend à être plus protecteur de la vie privée que le droit américain, mais l'étendue de cette protection peut varier quelque peu d'un pays à l'autre. L'anonymat est parfois considéré comme un droit lié à la vie privée, en particulier en ce qui concerne les données 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 prévoit 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 utilisateurs d'Internet de ne pas divulguer leur identité. En 2013, le Parlement européen a voté en faveur de l'adoption d'une nouvelle réglementation obligeant les entreprises à rendre anonymes les données personnelles collectées auprès des utilisateurs, après que la chancelière allemande Angela Merkel a persuadé les commissaires européens de soutenir une réglementation obligeant les entreprises du secteur de l'Internet à indiquer à qui elles transmettent les informations personnelles des utilisateurs. En 2014, la Cour de justice de l'Union européenne a statué que Google et d'autres fournisseurs de services Internet et de contenu devaient, dans certaines circonstances, accepter les demandes de désactivation d'anciens liens vers des informations, même véridiques, sur des personnes, afin qu'ils n'apparaissent pas dans les résultats de recherche relatifs à ces personnes (Moyakine, 2016).

Plus récemment, depuis mai 2018, le règlement **général sur la protection des données (RGPD)**, un règlement de l'UE sur la protection des données et de la vie privée pour tous les individus au sein de l'Union européenne (UE), vise à donner aux gens plus de contrôle sur leurs données personnelles et à unifier 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 stockées, et donne également aux individus le droit d'accéder à leurs données, de les faire corriger et de

les faire effacer dans certaines circonstances. Elle s'applique à toutes les organisations qui traitent des données à caractère personnel, qu'elles soient basées à l'intérieur ou à l'extérieur de l'UE.

En ce qui concerne l'anonymat en ligne, le GDPR encourage l'utilisation de la **pseudonymisation** et du **cryptage** pour réduire les risques pour les personnes concernées tout en aidant les responsables du traitement des données et les sous-traitants à respecter leurs obligations.[4] La législation européenne oblige les responsables du traitement à mettre en œuvre toutes les 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 à caractère personnel. Le règlement mentionne spécifiquement la pseudonymisation et le cryptage comme des instruments devant être déployés par les responsables du traitement et les sous-traitants dans le cadre du traitement des données à caractère personnel. Des législations européennes récentes, telles que la loi sur les marchés numériques, qui vise à créer un marché numérique équitable et concurrentiel dans l'UE en réglementant les "gatekeepers", 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 œuvre des garanties dans l'intérêt des personnes concernées. Celles-ci comprennent également la pseudonymisation et l'anonymisation des données à caractère personnel. Avec ces législations, l'anonymisation des données pourrait gagner en importance, mais le GDPR reste la norme en matière de traitement des données personnelles (Demircan, 2022).

Il convient de noter qu'en vertu du GDPR, si les données personnelles sont correctement anonymisées, elles ne sont plus considérées comme des données personnelles, de sorte que les dispositions du GDPR relatives à la protection des données personnelles ne s'appliquent pas aux données anonymisées.

[4] Nous définissons les "responsables du traitement" comme des personnes physiques ou morales, des autorités compétentes ou d'autres organismes qui déterminent les finalités et les moyens du traitement des données à caractère personnel. Les sous-traitants sont des personnes physiques ou morales, des autorités compétentes ou d'autres organismes qui traitent des données à caractère personnel pour le compte des responsables du traitement.

En conclusion, le droit à l'anonymat en ligne n'est pas explicitement mentionné dans la législation européenne en tant que droit autonome. Néanmoins, certaines affaires relatives à l'anonymat en ligne devant la Cour européenne des droits de l'homme montrent que la Cour considère l'anonymat comme un élément clé de la protection de la liberté d'expression en ligne dans l'Union européenne. Le 7 décembre 2021, la Cour a publié son arrêt dans l'affaire Standard Verlagsgesellschaft MBH c. Autriche (n° 3), dans lequel elle conclut que le tribunal autrichien a violé le droit à la liberté d'expression du requérant en exigeant de ce dernier qu'il révèle l'identité des personnes qui ont publié des commentaires prétendument diffamatoires sur son site web.

3.1.2 Approches restrictives de l'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 ligne 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 ou s'engagent dans des activités jugées menaçantes pour le régime.

A. Russie

Le gouvernement russe a adopté plusieurs mesures pour contrôler l'utilisation d'Internet par les citoyens. La "loi sur l'information, les technologies de l'information et la protection de l'information" (2006) oblige les fournisseurs de services en ligne à collecter et à conserver certaines informations sur leurs utilisateurs, notamment leur nom complet, leur adresse et d'autres informations permettant de les identifier. En 2016 et 2019, la "loi Yarovaya" et la "loi sur l'isolement de l'Internet" ont renforcé la loi précédente et exigé 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. En outre, il a été rapporté que le ministère russe de l'intérieur offrait près de 100 000 dollars pour des recherches sur la manière d'identifier les utilisateurs anonymes de Tor, qui masque les sources et les destinations de la navigation sur Internet et empêche les utilisateurs d'être suivis (Martin et Fargo, 2015).

B. Chine

La constitution chinoise garantit les libertés d'expression, d'association et de publication subordonnées au parti au pouvoir, mais le gouvernement chinois a fait de grands efforts pour empêcher l'anonymat et la participation à des sujets controversés grâce à un système complexe de filtrage, de blocage et d'enquête sur les sites web, les fournisseurs d'accès à Internet et les utilisateurs d'Internet. En 2011, 2012 et 2016, la Chine a pris plusieurs mesures visant à contrôler l'anonymat sur Internet, notamment en créant une nouvelle agence chargée de coordonner la réglementation d'Internet, en augmentant la pression sur les intermédiaires pour qu'ils "autocensurent" les contenus et les utilisateurs, et en renforçant les contrôles sur les médias sociaux. En 2012, le gouvernement chinois a adopté une politique obligeant les internautes à enregistrer leur nom réel auprès des fournisseurs de services afin d'aider ces derniers à mieux protéger les informations de leurs clients. Enfin, pour lever toute ambiguïté, la "loi sur la cybersécurité" et la "loi sur la sécurité de l'internet", promulguées en 2016 et 2017, imposent aux fournisseurs de services en ligne de stocker les données collectées en Chine sur des serveurs situés dans le pays et d'en accorder l'accès total aux autorités gouvernementales qui en font la demande. Cela démontre que le droit à l'anonymat en ligne en Chine n'est en fait pas garanti (Martin et Fargo, 2015).

3.2. 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 médias sociaux, les régulateurs ont commencé à s'intéresser davantage à l'élaboration de politiques susceptibles d'endiguer ces comportements indésirables sur les médias 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" (Rainie et al., 2017, p. 7). Cela a conduit certains

décideurs politiques à émettre des propositions visant à interdire ou à réglementer la possibilité pour les utilisateurs des plateformes de médias 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 médias sociaux (Baillie, 2021 ; Standing Committee on Social Policy and Legal Affairs, 2021, p. 31), 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 médias sociaux à leurs comptes, interdisant de fait les comptes anonymes de médias 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 médias 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.

3.2.1 Politique en matière de "nom réel

L'approche la plus radicale pour résoudre ce problème consisterait à rendre obligatoire l'utilisation de l'identité réelle des utilisateurs sur les plateformes de médias sociaux, en interdisant effectivement l'utilisation de pseudonymes. Cette position est déjà adoptée par certaines plateformes de médias sociaux, par exemple Facebook avec sa **politique du "vrai nom".** Toutefois, cette approche empiète considérablement sur les droits des utilisateurs de médias sociaux à opérer sous des alias ou des pseudonymes dans leurs activités en ligne, et Facebook a dû assouplir sa propre politique à la suite des critiques virulentes formulées par les associations de défense des libertés civiles dans le passé (Hern, 2015). Ce point de vue est partagé par un certain nombre d'organismes de réglementation, au premier rang desquels le Comité européen de protection des données et l'Agence française de protection des données, qui soutiennent tous deux que chaque utilisateur a le droit d'utiliser des pseudonymes

et devrait être libre de conserver plusieurs identités numériques, dont les attributs ne se chevauchent pas nécessairement et qui peuvent mettre en évidence différents aspects de l'identité d'une personne qu'elle ne souhaite pas nécessairement associer à son identité gouvernementale ou à d'autres identités numériques (CNIL, 2023, p. 10). Les avantages potentiels découlant d'une telle décision perturbatrice pourraient également ne pas compenser le préjudice infligé à la liberté d'expression en ligne. En fait, il convient de considérer que le fait d'imposer l'utilisation de "vrais" noms sur les plateformes de médias sociaux n'a pas été associé à une diminution absolue du harcèlement. Des plateformes telles que Facebook, qui appliquent la politique du "vrai nom" pour les utilisateurs, ne sont pas à l'abri du harcèlement en ligne, et si l'anonymat est certainement une force désinhibitrice qui peut encourager les abus chez certaines personnes, le véritable moteur de ces comportements semble être le manque de responsabilité perçue, plutôt que la possibilité de rester anonyme (Matias, 2017).

3.2.2 Pseudonymisation opposable

La mise en place d'une infrastructure réglementaire et technique permettant l'utilisation de **"pseudonymes opposables" a** été saluée comme une approche conciliante permettant de préserver un niveau élevé d'anonymat relatif pour les utilisateurs sur les plateformes de médias sociaux, tout en dotant les plateformes et les autorités publiques de nouveaux outils pour mieux appréhender la propagation des discours haineux et des campagnes de désinformation en ligne (Basdevant et al., 2022, p. 96).

Grâce à des outils cryptographiques tels que Zero Knowledge Proof (ZKP), les utilisateurs pourraient partager certains attributs de leur identité avec les plateformes de médias sociaux sans donner à ces dernières un accès direct aux informations utilisées pour la certification, soit par l'intermédiaire d'un tiers de confiance (par exemple, une banque) ou d'un portefeuille numérique personnel tel que celui actuellement développé par l'Union européenne (Commission européenne, 2023). Le service de certification de confiance répondrait à une requête des plateformes de médias sociaux par un attribut reconnaissant que l'individu à l'origine de la création du compte "est une personne" ou "est suffisamment âgé pour avoir accès au service", au lieu de communiquer un nom, un numéro de document d'identité ou une date de

naissance (Birch, 2019). S'il est élaboré en collaboration avec les gouvernements, ce service pourrait être conçu avec une procédure permettant aux autorités compétentes de passer outre le pseudonyme opposable et de le relier à l'identité d'une personne, ce qui faciliterait les recours juridiques contre les comportements illicites sur les plateformes de médias sociaux (Bennett & Beverton-Palmer, 2021).

En outre, la possibilité de vérifier que le propriétaire d'un compte est une personne physique créerait un nouveau niveau de contrôle offert aux utilisateurs sur les plateformes de médias sociaux. Ils pourraient par exemple définir leurs préférences sur les plateformes de médias sociaux afin d'éviter tout contact avec des comptes qui n'ont pas encore été vérifiés, et n'interagir qu'avec des utilisateurs dont ils sont certains qu'ils sont des personnes réelles. Cela permettrait de limiter l'impact que les réseaux de bots pourraient avoir sur les interactions des utilisateurs sur les principaux réseaux de médias sociaux. Donner plus de contrôle aux utilisateurs des plateformes de médias sociaux pour déterminer avec qui ils acceptent d'interagir a également le potentiel de réduire l'exposition des utilisateurs aux abus et au harcèlement : d'une part en les protégeant des utilisateurs qui ne sont pas passés par le processus de vérification et en permettant l'identification de ceux qui ont été vérifiés et qui adoptent des comportements illicites (Birch, 2019).

Bien que cette approche préserve la possibilité pour les utilisateurs de médias sociaux de rester anonymes vis-à-vis des autres utilisateurs et des plateformes elles-mêmes s'ils le souhaitent, les gouvernements devraient faire preuve de prudence dans leur approche de la mise en œuvre d'une telle solution. La possibilité pour les autorités publiques de "casser" les identifiants numériques pourrait limiter l'adoption généralisée d'une telle mesure et éventuellement susciter l'opposition des minorités qui considèrent qu'elle compromet leur capacité à s'exprimer à l'abri de tout contrôle extérieur ou de toute répression. Cette crainte pourrait être atténuée en concevant le système ZKP de manière à empêcher les tiers de confiance de savoir quelle plateforme de médias sociaux demande le jeton à des fins de vérification. Cela éliminerait la crainte des citoyens que le tiers de confiance soit en possession d'une liste reliant l'identité réelle d'une personne et le jeton utilisé pour vérifier l'identité de cette personne directement à la plateforme de médias sociaux pour laquelle il a été généré, tout en maintenant la

possibilité pour les autorités compétentes de créer ce lien si le besoin s'en fait sentir au cours d'une enquête justifiant cette intervention.

3. 4. Recommandations politiques et juridiques

Sur la base de l'analyse approfondie menée dans les sections précédentes, nous nous concentrons sur la section de notre mémoire consacrée aux recommandations politiques. Reconnaissant le rôle de l'Union européenne dans l'élaboration des politiques numériques, nous identifions **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.

4.1 L'anonymat doit être perçu dans le cadre plus large de la réglementation relative à la vie privée et à l'identité.

Défi 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.

4.2 Les solutions de vérification de l'identité numérique devraient être examinées en tant que levier potentiel pour réduire les abus en ligne, en consultation avec les parties prenantes.

4.

Défi politique :

L'idée de rendre obligatoire la **vérification de l'identité** des utilisateurs des plateformes de médias 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 médias 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 médias 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 grâce à l'effet Bruxelles (Gunst & De Ville, 2021, p. 439), 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 médias 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 (Bourreau, 2022). 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, nous formulons 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 médias 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 médias 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 médias sociaux. Le** cadre entourant les solutions de vérification d'identité devrait être élaboré par la Commission européenne en consultation avec les plateformes de médias 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 médias 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.

4.3 Garantir la protection de la vie privée grâce à l'anonymat

Défi politique :

notre 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 médias 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 défi politique se pose donc : *comment la Commission européenne peut-elle garantir et renforcer le respect de la vie privée garanti par l'anonymat sur les médias sociaux par le biais du GDPR 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 GDPR, évitant ainsi toute ré-identification possible (CIPL, 2021) ?*

Étant donné que l'anonymat et son application requièrent un niveau élevé d'expertise technique, ces recommandations combinent des mesures juridiques et techniques que nous conseillons à l'UE d'entreprendre. 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 ré-identification quasiment impossible (OCDE, 2023).
- **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 (Centre on Regulation in Europe, 2022).

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

- **Assurer une interaction cohérente entre le DMA et le GDPR.** Il est essentiel de fournir une interprétation cohérente et de maintenir une **approche réglementaire harmonisée entre le DMA et le GDPR.** 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 GDPR (Demircan, 2022), l'UE doit garantir que la DMA ne porte pas atteinte aux principes énoncés dans le GDPR et qu'elle ne s'en écarte pas.

Références

Aboujaoude, E., Savage, M.W., Starcevic, V., Salame, W.O., 2015. Cyberbullying : Review of an Old Problem Gone Viral. Journal of Adolescent Health 57, 10-18.

Allcott, H., Gentzkow, M., 2017. Social Media and Fake News in the 2016 Election (Médias sociaux et fausses nouvelles dans les élections de 2016). Journal of Economic Perspectives 31, 211-236.

Baillie, S. (2021) *Social Media Platforms (Identity Verification) Bill - Parliamentary Bills - UK Parliament*. Disponible à l'adresse : https://bills.parliament.uk/bills/3073

Barlow, J.P. (1996) A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation. Disponible à l'adresse : https://www.eff.org/pl/cyberspace-independence.

Basdevant, A., François, C. et Ronfard, R. (2022) *Mission exploratoire sur le métavers*, p. 116.

Bennett, A. et Beverton-Palmer, M. (2021) *Social Media Futures : How to Reconcile Anonymity, Abuse and Identity Online*, *Tony Blair Institute for Global Change*. Disponible à l'adresse : https://www.institute.global/insights/tech-and-digitalisation/social-media-futures-anonymity-abuse-and-identity-online.

Birch, D.G.W. (2019) " Inconnu, connu et vérifié | 15Mb ". Disponible à l'adresse : https://blog.dgwbirch.com/?p=562

Bode, N. et Makarychev, A. (2013) 'The New Social Media in Russia : Political Blogging by the Government and the Opposition', Problems of Post-Communism, 60(2), pp. 53-62.

Bourreau, M. (2022) *DMA : Obligations d'interopérabilité horizontale et verticale*. Centre sur la régulation en Europe.

Cadec, A. (2021) *Proposition de loi instituant une Autorité de contrôle de l'identité numérique*.

Cadwalladr, C. (2012) "Anonymous : behind the masks of the cyber insurgents", The Observer, 8 septembre. Disponible à l'adresse : https://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents

CIPL (2019). Faire le pont entre le DMA et le GDPR.

CNIL (2023) *L'identité numérique*. Dossier thématique. Paris : CNIL, p. 20.

De Filippi, P. (2016) 'The Interplay between Decentralization and Privacy : The Case of Blockchain Technologies'. Rochester, NY. Disponible à l'adresse : https://papers.ssrn.com/abstract=2852689 (consulté le 13 avril 2023).

Demircan, M., 2022. Le DMA et le GDPR : Comprendre les dispositions relatives à l'accumulation, à l'utilisation croisée et au partage des données.

Demircan, Muhammed. Le DMA et le GDPR : Making Sense of Data Accumulation, Cross-Use and Data Sharing Provisions". *Vrije Universiteit Brussel*, décembre 2022

EUROJUST (2023) New strike against encrypted criminal communications with dismantling of Exclu tool | Eurojust | European Union Agency for Criminal Justice Cooperation. Disponible à l'adresse : https://www.eurojust.europa.eu/news/new-strike-against-encrypted-criminal-communications-dismantling-exclu-tool (consulté le 13 avril 2023).

Commission européenne (2021) Recommandation de la Commission du 3.6.2021.

Commission européenne (2023) *Identité numérique européenne*. Disponible à l'adresse : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (consulté le 15 avril 2023).

Contrôleur européen de la protection des données (2023) *Avis sur la proposition de loi relative à l'Europe interopérable*.

Feher, K. (2021) 'Digital identity and the online self : Footprint strategies - An exploratory and comparative research study", Journal of Information Science, 47(2), pp. 192-205. Disponible à l'adresse : https://doi.org/10.1177/0165551519879702.

Ferrara, E., 2020. Quels types de conspirations COVID-19 sont alimentés par des Twitter Bots ? FM.

Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A., 2016. The Rise of Social Bots. Commun. ACM 59, 96-104.

Floridi, L. 2005. "The Ontological Interpretation of Informational Privacy", Ethics and Information Technology, 7(4), pp. 185-200. Disponible à l'adresse : https://doi.org/10.1007/s10676-006-0001-7.

Floridi, L. 2014. La 4e révolution : comment l'infosphère remodèle la réalité humaine. Première édition. New York ; Oxford : Oxford University Press.

Floridi, L., 2005. The Ontological Interpretation of Informational Privacy (Interprétation ontologique de la confidentialité des informations). Ethics Inf Technol 7, 185-200.

Frye, N.E., Dornisch, M.M., 2010. Quand la confiance ne suffit-elle pas ? The role of perceived privacy of communication tools in comfort with self-disclosure. Computers in Human Behavior, Advancing Educational Research on Computer-supported Collaborative Learning (CSCL) through the use of gStudy CSCL Tools 26, 1120-1127.

Gottfried, J., Shearer, E., 2016. News use across social media platforms. Livre blanc, Pew Research Center.

Gunst, S., De Ville, F., 2021. L'effet Bruxelles : comment le GDPR a conquis la Silicon Valley. EERR 26, 437-458. https://doi.org/10.54648/EERR2021036

Nissenbaum, H., 1999. The Meaning of Anonymity in an Information Age, The Information Society, 15:2, 141-144.

Hern, A. 2015. Facebook relaxes "real name" policy in face of protest", *The Guardian*, 2 novembre. Disponible à l'adresse : https://www.theguardian.com/technology/2015/nov/02/facebook-real-name-policy-protest.

Howard, P.N., Duffy, A., Freelon, D., Hussain, M.M., Mari, W. & Maziad, M., 2011. Opening Closed Regimes : Quel a été le rôle des médias sociaux pendant le printemps arabe ?

Koehler, D. 2014. Le radical en ligne : Individual Radicalization Processes and the Role of the Internet. Journal for Deradicalization 116-134.

Kramer, J. 2022. Data Access Provisions in the DMA (Dispositions relatives à l'accès aux données). *Centre on Regulation in Europe - Issue Paper Novembre 2022*

Lawlor, A., Kirakowski, J., 2014. Online support groups for mental health : Un espace pour défier l'auto-stigmatisation ou un moyen d'évitement social ? Computers in Human Behavior 32, 152-161.

Martin, Jason A., et Anthony L. Fargo. L'anonymat en tant que droit légal : Where and Why It Matters". *16 N.C. J.L. & Tech. 311*, 2015.

Matias, J.N. 2017. The Real Name Fallacy", *Coral by Vox Media*, 3 janvier. Disponible à l'adresse : https://coralproject.net/blog/the-real-name-fallacy/

McAdams, D.P. 2001. The Psychology of Life Stories", Review of General Psychology, 5(2), pp. 100-122. Disponible à l'adresse : https://doi.org/10.1037/1089-2680.5.2.100.

Meleagrou-Hitchens, A., Alexander, A., Kaderbhai, N., 2017. L'impact des technologies de communication numérique sur la radicalisation et le recrutement. International Affairs 93, 1233-1249.

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.

Mühle, A. et al. (2018) " A survey on essential components of a self-sovereign identity ", Computer Science Review, 30, pp. 80-86. Disponible à l'adresse : https://doi.org/10.1016/j.cosrev.2018.10.002.

Nathaniel A. Persily, 2019. Le défi d'Internet pour la démocratie : Définir le problème et évaluer les réformes (2019).

Nissenbaum, H., 2004. Privacy as Contextual Integrity (La vie privée en tant qu'intégrité contextuelle). Washington Law Review 79.

Nissenbaum, H., 2009. Privacy in Context : Technology, Policy, and the Integrity of Social Life. Stanford University Press.

OCDE, 2023. Technologies émergentes renforçant la protection de la vie privée. Approches réglementaires et politiques actuelles. *Documents de l'OCDE sur l'économie numérique*

Patchin, J.W., Hinduja, S., 2010. Cyberbullying and Self-Esteem*. Journal of School Health 80, 614-621.

Pfitzmann, A. et al. 2007. Anonymat, dissociabilité, inobservabilité, pseudonymat et gestion de l'identité - une proposition consolidée de terminologie".

Rainie, L. *et al.* 2017. *L'avenir de la liberté d'expression, des trolls, de l'anonymat et des fausses nouvelles en ligne*. Pew Research Center. Disponible à l'adresse : https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/.

Salmony, M. (2018) "Repenser l'identité numérique", *Journal of Payments Strategy and Systems*, 12, pp. 40-57.

Scott, S.V. et Orlikowski, W.J. (2014) 'v', MIS Quarterly, 38(3), pp. 873-894.

Shahi, G.K., Dirkson, A., Majchrzak, T.A., 2021. Une étude exploratoire de la désinformation COVID-19 sur Twitter. Online Social Networks and Media 22, 100104.

Shao, C., Ciampaglia, G.L., Varol, O., Yang, K., Flammini, A., Menczer, F., 2018. La diffusion de contenus de faible crédibilité par les bots sociaux. Nat Commun 9, 4787.

Shao, C., Ciampaglia, G.L., Varol, O., Yang, K.-C., Flammini, A., Menczer, F., 2018. La diffusion de contenus de faible crédibilité par les bots sociaux. Nat Commun 9, 4787.

Comité permanent de la politique sociale et des affaires juridiques, 2021. *Enquête sur la violence familiale, domestique et sexuelle*. Canberra : Parlement du Commonwealth d'Australie, p. 471.

Suler, J., 2004. The Online Disinhibition Effect. CyberPsychology & Behavior 7, 321-326.

Sullins, Lauren L. " "Phishing" for a solution : domestic and international approaches to decreasing online identity theft ", Emory international law review. 2006, vol.20 no 1. p. 397-.

Wallace, K.A. 1999. Anonymity", Ethics and Information Technology, 1(1), pp. 21-31. Disponible à l'adresse : https://doi.org/10.1023/A:1010066509278.

Whitman, J.Q. 2004. The Two Western Cultures of Privacy : Dignity versus Liberty", The Yale Law Journal, 113(6), pp. 1151-1221. Disponible à l'adresse : https://doi.org/10.2307/4135723.

Whittaker, E., Kowalski, R.M., 2015. Cyberbullying Via Social Media. Journal of School Violence 14, 11-29.

Zuboff, S., 2015. Big Other : Surveillance Capitalism and the Prospects of an Information Civilization (Le capitalisme de surveillance et les perspectives d'une civilisation de l'information).

A propos des auteurs :

Lorenzo Ancona a une formation en sciences politiques et en communication numérique et effectue actuellement un stage en tant qu'analyste de la politique numérique. Il s'intéresse au potentiel de transformation de la numérisation en tant que moyen de renforcer la démocratie et de catalyser la participation des citoyens. Ses recherches portent sur l'intersection de la technologie et des valeurs sociétales, la transformation numérique pour le gouvernement et l'innovation pour la démocratie.

Wiktor Samek est étudiant en deuxième année de master dans le domaine du numérique, des nouvelles technologies et des politiques publiques et stagiaire à l'unité "Gouvernement numérique et données" de l'OCDE. Avec une formation en sciences politiques et en droit, il s'intéresse principalement à l'impact de la technologie sur le développement des identités politiques contemporaines, à l'implication de l'État dans l'économie numérique et au concept d'identité numérique.

Avec une formation en économie et en sociologie, Arnau Marti poursuit actuellement un master en politiques publiques et innovation à l'École d'affaires publiques de Sciences Po. **Arnau Marti** poursuit actuellement un master en politiques publiques et innovation à l'École d'affaires publiques de Sciences Po. Après avoir travaillé comme assistant de recherche et membre d'équipes de programmes gouvernementaux en Amérique latine, il s'intéresse à l'innovation en matière de politiques macroéconomiques. Ses dernières recherches portent sur la transition énergétique, le commerce international durable et la finance.

Gabriel Karl a une formation en relations internationales, en politique comparée et en affaires européennes. Diplômé du programme de double diplôme entre Sciences Po et l'Université de Columbia, il a pu s'engager dans des perspectives à la fois américaines et européennes sur une variété de sujets centraux pour les affaires internationales. Il s'intéresse particulièrement à la transformation numérique des gouvernements et à l'impact des données ouvertes sur les politiques publiques.

À propos de la chaire Digital, gouvernance et souveraineté:

La Chaire Digital, Gouvernance et Souveraineté de Sciences Po a pour mission de créer un forum réunissant des entreprises techniques, des universitaires, des décideurs politiques, des acteurs de la société civile, des incubateurs de politiques publiques ainsi que des experts de la régulation numérique. Hébergée par l'Ecole d'affaires publiques, la Chaire adopte une approche multidisciplinaire et holistique pour rechercher et analyser les transformations économiques, juridiques, sociales et institutionnelles induites par l'innovation numérique. La Chaire Digital, Gouvernance et Souveraineté est présidée par **Florence G'sell**, professeur de droit à l'Université de Lorraine, maître de conférences à l'Ecole d'affaires publiques de Sciences Po.

Les activités de la Chaire sont soutenues par :