Manque de contrôle sur la dissémination de l'identité numérique sur internet

Alexandre Gomes

Jathavan Thamaraichelvan

Kevin Lopes Fernandes

Mai 2025

Table des matières

1 | Introduction

À l'ère du numérique, notre présence en ligne ne se résume plus à de simples traces éparses. Elle constitue désormais une véritable extension de notre identité. Pourtant, cette identité numérique, produite au fil de nos interactions quotidiennes avec les technologies connectées, échappe de plus en plus à notre contrôle. Du clic anodin à l'algorithme prédictif, en passant par les plateformes, les objets connectés ou les services administratifs, chaque fragment de donnée contribue à forger une représentation de nous-mêmes. Ce constat soulève une question centrale : dans quelle mesure l'individu peut-il encore maîtriser la circulation et l'usage de ses données dans un système numérique dominé par des logiques d'optimisation, de rentabilité et de centralisation ? À travers une approche systémique, cette étude propose d'explorer les mécanismes profonds qui rendent la dissémination de l'identité numérique si difficile à encadrer, les conséquences multiples de ce phénomène sur la société, ainsi que les leviers de transformation envisageables.

2 | L'identité numérique dans son contexte

L'identité numérique désigne l'ensemble des données, traces, informations et représentations qu'un individu génère volontairement ou non dans l'environnement numérique. Elle est constituée à la fois de données déclaratives simples (nom, âge, adresse e-mail), de données comportementales (clics, temps de lecture, géolocalisation) et de données calculées ou déduites par les systèmes algorithmiques (préférences, risques, tendances d'achat). Contrairement à une identité civile qui se veut « fixe » et centralisée, l'identité numérique est fragmentée, dynamique et contextuelle. Elle varie selon les plateformes, les services utilisés et les intentions des acteurs qui l'exploitent. Floridi (2011) parle ainsi d'une construction socio-technique façonnée par les interactions avec les infrastructures numériques, tandis que Zuboff (2019) souligne que cette identité est souvent captée et transformée à des fins de prédiction comportementale. L'identité numérique ne se limite donc pas à ce que nous disons de nous-mêmes, elle inclut ce que les machines calculent et imposent comme représentation de notre personne. Dès lors, elle devient un enjeu central dans l'environnement numérique contemporain.

Le contexte de développement rapide des technologies numériques, combiné à l'omniprésence des plateformes dans la vie quotidienne a profondément modifié la manière dont les identités

se forment et sont utilisées. Loin d'être une simple extension administrative ou sociale de la personne, l'identité numérique est aujourd'hui un levier économique stratégique pour les entreprises, un outil de gouvernance pour les États et un vecteur d'inégalités pour les populations les plus vulnérables. Les utilisateurs se trouvent souvent impuissants face à l'opacité des systèmes de collecte et de traitement des données. Le consentement pourtant censé garantir une certaine autonomie décisionnelle devient de plus en plus symbolique, voire illusoire. Pendant ce temps, les régulations peinent à suivre la vitesse des innovations.

C'est dans cette tension entre innovation technologique, exploitation économique et besoin de souveraineté individuelle que s'inscrit la problématique du manque de contrôle sur la dissémination de l'identité numérique.

3 | Approches systémiques

3.1 | Carte du système

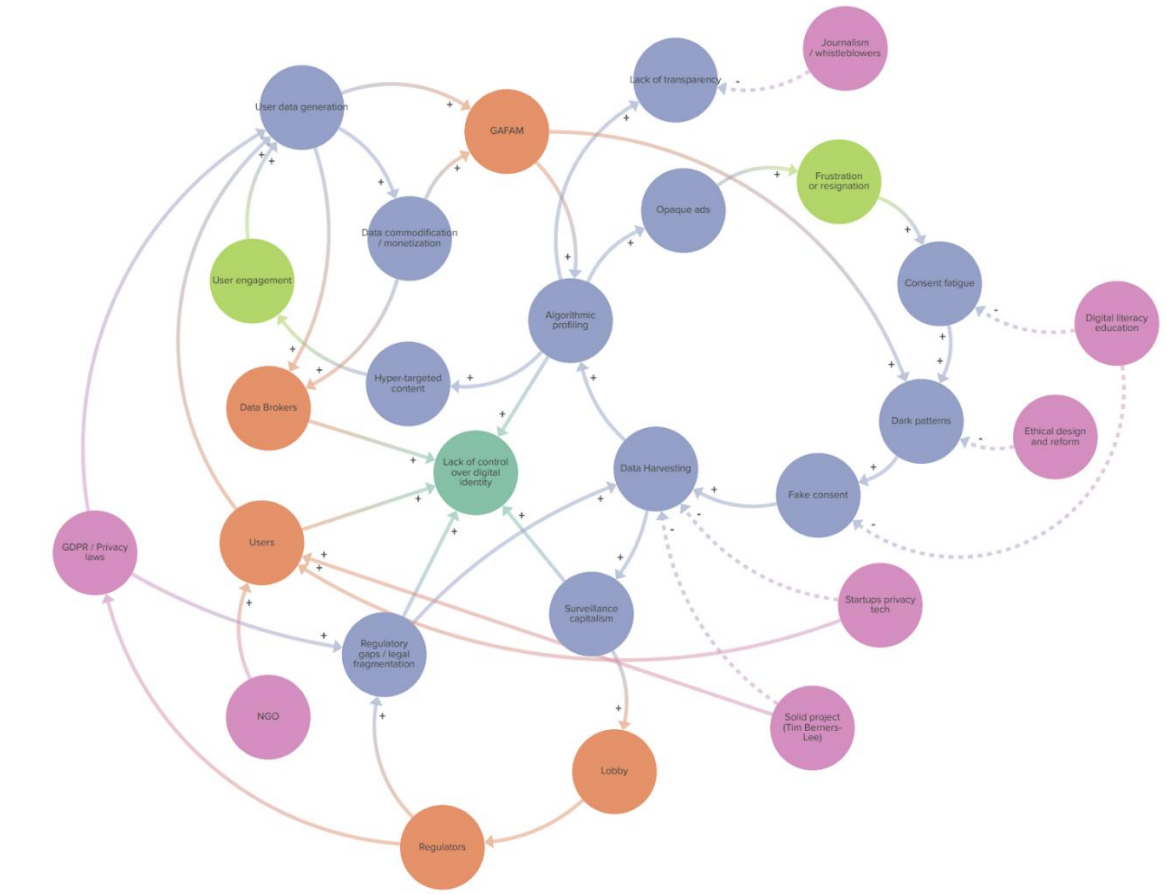

Figure 1 : Carte du système

(https://embed.kumu.io/73a2daa2105b6ec68b349aebec5b6090#systems-map-of-the-dissemination-of-the-digital-identity)

3.2 | Modèle de l'iceberg

Pour comprendre les mécanismes invisibles qui alimentent la dissémination non contrôlée de l'identité numérique, il est essentiel d'adopter une lecture en profondeur du système. Le modèle de l'iceberg permet d'analyser cette problématique au-delà des symptômes visibles, en révélant les dynamiques structurelles et culturelles qui la soutiennent.

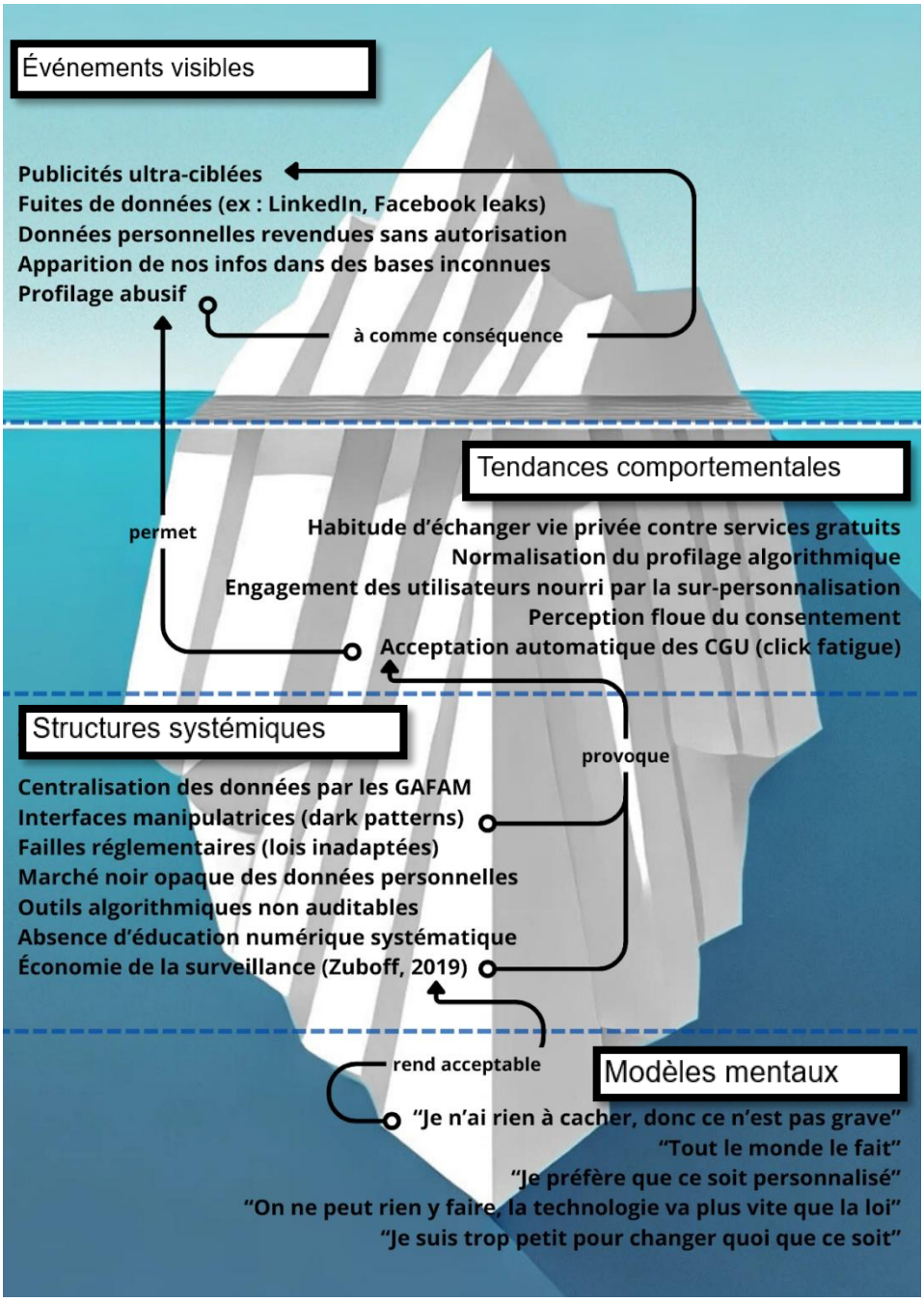

Figure 2 : Modèle de l'Iceberg dans son contexte

3.3 | Carte des acteurs

Afin de mieux comprendre les dynamiques de pouvoir et les relations qui structurent le système, une cartographie des parties prenantes a été réalisée. Cette carte met en évidence les rôles et les interactions des principaux acteurs impliqués dans la collecte, l'exploitation et la régulation des données personnelles.

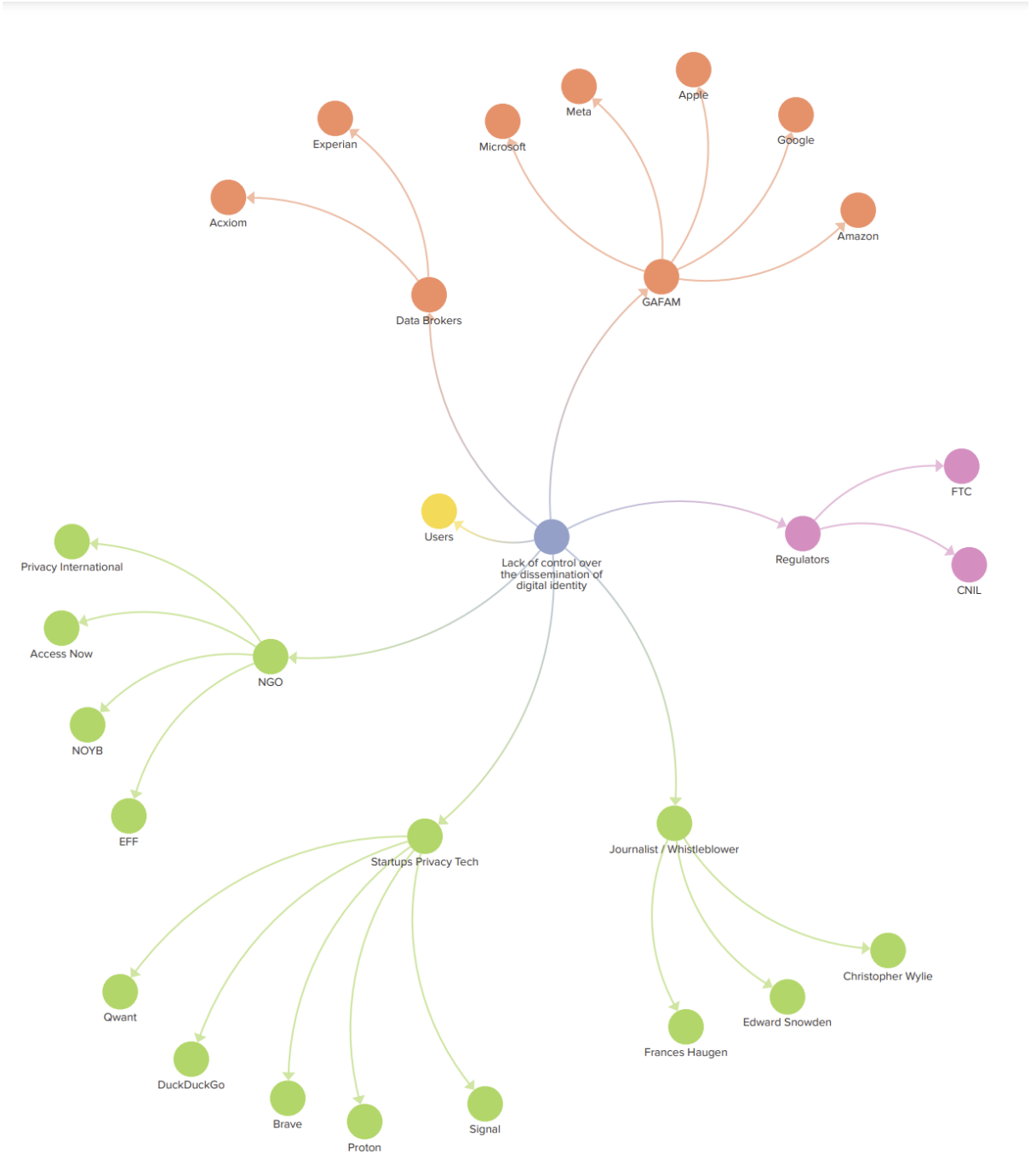

Figure 3 : Carte des acteurs

4 | Analyse du système : manque de contrôle sur la dissémination de l'identité numérique sur internet

L'absence de contrôle sur l'identité numérique n'est pas le fruit d'un dysfonctionnement isolé, mais le résultat d'un système cohérent et auto-renforcé. Ce chapitre passe en revue les mécanismes invisibles qui rendent ce système résilient, opaque et profondément enraciné dans nos usages quotidiens. Différents modèles systémiques sont relevés : l'asymétrie de pouvoir, les boucles de rétroaction, l'architecture algorithmique et la fragilité des régulations.

Dans un premier temps, la structure du système repose sur une asymétrie fondamentale. Les individus génèrent des données sans savoir ni comment elles sont utilisées, ni par qui. Alors qu'en face, un nombre restreint d'acteurs comme des plateformes numériques, des courtiers en données ou encore des entreprises publicitaires détiennent la capacité technique, juridique et financière d'exploiter ces données à grande échelle. Andrejevic (2014) décrit le phénomène par « big data divide », une fracture entre les producteurs de données (les utilisateurs) et ceux qui les exploitent. Ce déséquilibre est renforcé par la centralisation du Web autour de plateformes comme Google, Meta ou Amazon qui captent les données, dictent les normes d'usage et contrôlent les infrastructures.

Dans un deuxième temps, loin d'être de simples acteurs passifs, les algorithmes filtrent, hiérarchisent et orientent les contenus visibles par les utilisateurs. Cette personnalisation dynamique et invisible repose sur une multitude de signaux comportementaux (clics, pauses, likes, localisations) qui alimentent des profils d'identité. Il y a un réel manque de transparence quant à ces algorithmes. Tufekci (2015) qualifie cette logique de « computational agency ». Les algorithmes prennent des décisions ayant un impact direct sur la perception de soi et le comportement des usagers. En l'absence d'audit externe, ces systèmes fonctionnent comme des boîtes noires impossibles à contester.

Pour continuer, le système numérique peut être décrit par des boucles auto-renforcées. Comme la boucle suivante :

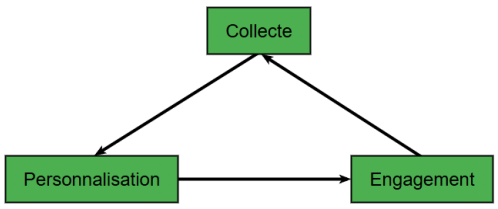

Figure 4 : Exemple de boucle

En effet, plus l'utilisateur interagit, plus il génère de données qui améliorent la précision des contenus suggérés ce qui l'incite à interagir davantage. Ce cycle d'optimisation continue repose sur des mécanismes dopaminergiques (Sherman et al., 2018) qui exploitent la psychologie de la récompense. En parallèle, ces données permettent des inférences de plus en plus précises sur les préférences, opinions ou vulnérabilités des utilisateurs (Kosinski et al., 2013). Cette capacité de prédiction renforce les campagnes de micro-ciblage, notamment dans la publicité. Comme l'observe Andrejevic (2014), les plateformes anticipent un comportement, le favorisent par leur design et l'observent ensuite comme validation.

Aussi, dans le fonctionnement actuel du système, la notion de consentement éclairé tend à devenir une illusion. Les interfaces sont conçues pour fatiguer ou distraire l'utilisateur, l'incitant à accepter toutes conditions par défaut. Mathur et al. (2021) décrivent ces pratiques sous le terme de "dark patterns" désormais monnaie courante sur les sites et applications. Même les utilisateurs les plus soucieux de leur vie privée se retrouvent pris dans des mécanismes de choix trompeurs où l'option par défaut devient une stratégie commerciale.

Enfin, face à ces logiques systémiques, les cadres réglementaires peinent à suivre. Le RGPD (Règlement Général sur la Protection des Données) représente une avancée importante mais son application est freinée par des interfaces opaques, une faible transparence technique et des inégalités d'accès au recours. La CNIL et la Commission européenne révèlent que les dispositifs actuels sont dépassés par la vitesse des transformations numériques. Les régulateurs manquent de moyens tandis que les plateformes sur lesquelles transitent les données maîtrisent parfaitement l'art de détourner les contraintes légales.

5 | Conséquences visibles : symptômes d'un système défaillant

La dissémination non contrôlée de l'identité numérique produit des effets profonds sur les individus, les institutions et la société dans son ensemble. Ces conséquences sont les manifestations directes de la logique structurelle décrite dans le chapitre précédent. Elles fragilisent l'autonomie, menacent la vie privée, creusent les inégalités et révèlent la vulnérabilité systémique du numérique contemporain.

Floridi (2011) souligne que l'identité numérique devient une construction fragmentée et façonnée par les plateformes, échappant de plus en plus à la volonté des utilisateurs. Cela altère

la capacité à se représenter soi-même dans l'espace numérique. À grande échelle, la surveillance est devenue une condition implicite de l'accès aux services numériques. Selon Zuboff (2019), le capitalisme de surveillance transforme les traces comportementales en prédictions commerciales sans que l'utilisateur en perçoive toujours les mécanismes et cette surveillance s'intègre dans les gestes du quotidien (activer un GPS, publier une photo, consulter une vidéo). Progressivement, l'idée d'une vie numérique sans surveillance devient impensable.

En outre, tous les individus ne sont pas égaux face aux risques liés à la dissémination de l'identité numérique. Seuls ceux qui disposent de ressources techniques ou juridiques peuvent exercer un certain contrôle. Les autres, souvent jeunes, précaires ou peu alphabétisés numériquement sont les plus exposés. L'OCDE et l'Eurobaromètre (Commission européenne) confirment que la compréhension réelle des mécanismes de protection des données reste minoritaire même si la sensibilisation générale progresse.

Au niveau économique et institutionnel, les violations de données deviennent une menace organisationnelle majeure. Selon IBM (International Business Machines Corporation) une fuite de données coûte plus de 4,45 millions de dollars. Comme les données passent souvent par des intermédiaires (comme les revendeurs de données), elles deviennent plus exposées ce qui rend la protection beaucoup plus difficile.

En dernier lieu, un paradoxe central persiste. Bien que la méfiance envers les plateformes augmente (Privacy International), les usages numériques ne reculent pas et il n'y a pas de réel changement de comportement. Ce paradoxe traduit une forme de résignation sociale où les individus s'inquiètent mais continuent à céder leurs données faute d'alternatives ou de compréhension.

6 | Interventions existantes et leurs limites

De nombreuses initiatives ont émergé pour tenter de répondre au problème du manque de contrôle de la diffusion de l'identité numérique. Cependant, leur impact reste limité en raison de plusieurs facteurs tels que le manque de cohérence systémique, des capacités de mise en œuvre inégales ou encore d'une résistance structurelle du modèle économique dominant.

Face à la dissémination incontrôlée de l'identité numérique, plusieurs initiatives ont émergé au cours de la dernière décennie. Celles-ci traduisent une prise de conscience croissante du

problème mais leurs effets restent encore limités face à la profondeur des logiques systémiques en jeu.

6.1 | Régulation juridique

Le RGPD adopté par l'Union européenne constitue sans doute l'une des avancées les plus notables dans la tentative de reconquérir une forme de souveraineté numérique. Il garantit plusieurs droits fondamentaux aux utilisateurs, tels que le consentement explicite, le droit à l'effacement, la portabilité des données ou encore la transparence dans les traitements. Cependant, la mise en œuvre effective de ces principes se heurte à de nombreuses limites. En pratique, les plateformes contournent les obligations légales en s'appuyant sur des interfaces manipulatoires appelées « dark patterns », qui rendent l'acceptation des conditions d'utilisation plus simple que leur refus (Mathur et al., 2021). Ce déséquilibre annule la portée du consentement. Par ailleurs, les mécanismes de sanction prévus par le RGPD se révèlent souvent lents, coûteux et peu dissuasifs. Les autorités de protection des données telles que la CNIL en France manquent de ressources suffisantes pour exercer un contrôle à grande échelle (CNIL, 2024). Sur le plan international, les régimes juridiques sont encore plus hétérogènes. Aux États-Unis, par exemple, la Federal Trade Commission (FTC) joue un rôle de régulation mais sans cadre équivalent au RGPD ce qui limite l'efficacité des actions coordonnées au niveau mondial (FTC, 2024).

6.2 | Innovations technologiques

Certaines initiatives technologiques tentent d'offrir des alternatives concrètes à l'économie de la surveillance. C'est notamment le cas du projet Solid porté par Tim Berners-Lee (2021), qui propose une architecture décentralisée permettant aux individus de stocker leurs données personnelles dans des PODS (Personal Online Data Store) qu'ils contrôlent eux-mêmes. Ce modèle redonne une véritable souveraineté numérique mais son déploiement reste limité par le manque de soutien institutionnel, de financements durables et de visibilité auprès du grand public. D'autres acteurs de la « privacy tech » tels que les navigateurs Brave, les moteurs de recherche éthiques comme Qwant ou DuckDuckGo, ou encore des entreprises comme Proton proposent des outils respectueux de la vie privée. Pourtant, ces solutions peinent à s'imposer dans un marché numérique largement dominé par les GAFAM (Google, Apple, Facebook,

Amazon, Microsoft) dont les modèles économiques sont solidement ancrés et subventionnés par la captation de données.

6.3 | Éducation au numérique

L'un des leviers les plus prometteurs à long terme réside dans l'éducation. La CNIL a développé plusieurs ressources pédagogiques pour sensibiliser les élèves aux enjeux de la protection des données personnelles et de l'identité numérique. Toutefois, cette éducation reste peu systématisée et inégalement intégrée dans les programmes scolaires. Elle dépend encore trop souvent de la motivation individuelle des enseignants ou de l'implication locale des collectivités. À l'échelle internationale, très peu d'États ont institutionnalisé une éducation aux droits numériques réellement effective. Or, sans cette formation citoyenne, les droits formels inscrits dans les textes de loi risquent de rester inaccessibles à une majorité d'utilisateurs.

6.4 | Mobilisation de la société et coordination mondiale

Des organisations non gouvernementales telles que Privacy International ou Access Now jouent un rôle essentiel dans la dénonciation des abus et la sensibilisation du public. De même, des lanceurs d'alerte comme Edward Snowden ou Frances Haugen ont révélé l'ampleur des pratiques de surveillance systémique, provoquant des débats publics majeurs. Néanmoins, ces interventions ont souvent un effet ponctuel, concentré autour de moments de crise, sans parvenir à déclencher un changement structurel durable.

Enfin, des organisations internationales comme l'OCDE, le Conseil de l'Europe ou les Nations Unies ont élaboré des principes directeurs en matière de responsabilité algorithmique, de respect de la vie privée ou encore de transparence des systèmes d'intelligence artificielle. Si ces cadres éthiques constituent des avancées importantes, ils sont non contraignants et reposent sur la seule bonne volonté des États ou des entreprises. Il n'existe à ce jour aucune autorité mondiale dotée d'un pouvoir effectif pour réguler les pratiques des grandes plateformes opérant au-delà des frontières nationales.

7 | Leviers de changement et recommandations

Transformer en profondeur le système actuel de dissémination incontrôlée des identités numériques exige une approche systémique, intégrée et ambitieuse. Cette transformation ne peut se limiter à des ajustements techniques ou juridiques isolés. Elle requiert une redéfinition globale des équilibres de pouvoir, des structures technologiques et des pratiques citoyennes. Plusieurs leviers complémentaires peuvent ainsi être mobilisés pour renforcer le contrôle des utilisateurs sur leurs données personnelles, tout en orientant l'architecture numérique vers des logiques éthiques et durables.

7.1 | Rééquilibrer le pouvoir dans l'écosystème numérique

L'une des causes fondamentales de la dissémination incontrôlée des identités numériques réside dans l'asymétrie massive entre les plateformes numériques et les utilisateurs. Pour y remédier, des réformes structurelles sont nécessaires à l'échelle nationale et internationale. Tout d'abord, il convient de renforcer les régulations internationales en matière de protection des données, d'intelligence artificielle et de ciblage comportemental. Des cadres juridiques plus contraignants doivent être adoptés pour encadrer les pratiques des entreprises transnationales souvent situées hors de portée des régulations nationales. L'OCDE souligne ainsi l'urgence de créer des normes globales applicables à la fois au transfert de données et à l'utilisation algorithmique des informations personnelles.

Ensuite, les autorités de protection des données telles que les CNIL nationales, le Contrôleur européen de la protection des données (EDPS), ou la Federal Trade Commission (FTC) doivent être dotées de moyens renforcés. Cela inclut des capacités d'enquête accrues, un pouvoir de sanction dissuasif ainsi qu'une coopération transfrontalière efficace pour faire face à la nature globalisée des flux de données (FTC, 2024). Par ailleurs, il devient impératif d'interdire les pratiques de manipulation des interfaces qui exploitent les biais cognitifs des utilisateurs pour les amener à consentir sans réelle compréhension. Leur interdiction dans les législations nationales, comme recommandé par Mathur et al. (2021), constituerait un pas décisif vers une meilleure protection des choix individuels. Aussi, le ciblage comportemental doit être encadré voire interdit. Comme l'a montré Zuboff (2019), ces pratiques alimentent des formes de manipulation de masse incompatibles avec les principes démocratiques.

7.2 | Construire des outils respectueux de la vie privée

Le deuxième levier concerne la technologie elle-même. Il est indispensable de soutenir la recherche et l'innovation éthique pour offrir des alternatives concrètes à l'économie de la surveillance. Des projets tels que Solid offrent un exemple inspirant où les utilisateurs peuvent gérer directement l'accès à leurs données personnelles grâce à une architecture décentralisée. De même, il est essentiel de soutenir le développement d'outils open source axés sur la protection de la vie privée comme des navigateurs sans pistage, des plateformes coopératives ou des applications sans publicité ni collecte intrusive de données.

7.3 | Vers une autonomie des utilisateurs

Aucune transformation durable ne peut s'opérer sans une autonomisation active des citoyens. Il s'agit de construire une culture numérique critique et participative dès le plus jeune âge. Cela passe par l'institutionnalisation de l'éducation aux droits numériques dans les programmes scolaires. Comme le souligne la CNIL, il est crucial que les jeunes comprennent le fonctionnement des plateformes et les droits dont ils disposent pour protéger leur identité en ligne. Des mécanismes de participation citoyenne doivent également être développés et il importe aussi de valoriser les initiatives de sensibilisation.

Enfin, la mise en place d'indicateurs de confiance serait un signal fort. Cela pourrait prendre la forme de certifications éthiques, de labels ou de transparence sur le traitement de l'identité numérique par les plateformes.

7.4 | Vers une transformation systémique

Ces leviers ne peuvent fonctionner de manière isolée. Ils doivent être activés conjointement dans une logique de transformation systémique. Cela implique un rééquilibrage progressif sur plusieurs niveaux d'action interdépendants :

Niveau d'action	Leviers clés
Institutionnel	Régulation transnationale, sanctions efficaces, transparence des algorithmes
Technologique	Décentralisation, auditabilité, « privacy by design »
Citoyen	Éducation, participation, contrôle effectif des usages

Tableau 1 : Niveaux d'action et leviers

Un numérique plus éthique centré sur l'humain ne pourra émerger que si les modèles économiques, les infrastructures techniques et les rapports sociaux sont repensés à partir d'un principe fondamental : les données comme prolongement de la personne humaine. C'est à cette condition que les individus pourront retrouver un véritable contrôle sur leur identité numérique dans un environnement numérique devenu équitable et transparent.

8 | Conclusion

La dissémination non contrôlée de l'identité numérique n'est ni accidentelle, ni marginale. Elle est le produit logique d'un écosystème structuré autour de l'extraction de données comme ressource stratégique. Dans un environnement où la surveillance est devenue la condition d'accès aux services numériques, les individus voient leur autonomie se réduire au profit d'acteurs puissants. Cette évolution n'est pas sans conséquence car elle fragilise la souveraineté individuelle, accentue les inégalités d'accès à la vie privée et diminue la confiance dans les infrastructures numériques elles-mêmes. Pour autant, cette situation n'est pas irréversible. L'analyse systémique démontre que les racines du problème peuvent être attaquées par des leviers profonds et articulés. Cela suppose une transformation simultanée sur plusieurs fronts (juridique, technologique, éducatif et culturel). Le renforcement des régulations internationales,

la création d'outils respectueux de la vie privée, l'autonomisation des citoyens et la redéfinition des modèles économiques sont autant de conditions nécessaires à la reconstruction d'un numérique plus éthique. Mais cette transformation ne peut reposer uniquement sur des ajustements périphériques. Elle exige une remise en question des paradigmes actuels où les données sont perçues comme un bien marchand plutôt que comme une extension de la personne humaine. À ce titre, la protection de l'identité numérique n'est pas qu'une question technique, elle est profondément politique car elle touche à la capacité de chacun à interagir et se représenter dans l'espace numérique sans subir l'exploitation ou la manipulation. Redonner aux individus un contrôle effectif sur leur identité numérique, c'est œuvrer à une société où les infrastructures numériques servent les libertés fondamentales plutôt que de les contraindre. C'est aussi poser les fondations d'un futur numérique plus juste, plus transparent et centré sur l'humain. Un futur où la technologie est au service de la personne et non l'inverse.

9 | Bibliographie

Andrejevic M (2014) Big Data, Big Questions| The Big Data Divide. *International Journal of Communication* 8(0). 0: 17.

Floridi L (2011) The Construction of Personal Identities Online. *Minds and Machines* 21(4): 477-479. DOI : 10.1007/s11023-011-9254-y.

Kosinski M, Stillwell D et Graepel T (2013) Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America* 110(15): 5802-5805. DOI : 10.1073/pnas.1218772110.

Mathur A, Kshirsagar M et Mayer J (2021) What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 7 mai 2021, p. 1-18. CHI '21. Association for Computing Machinery. DOI : 10.1145/3411764.3445610.

Sherman LE, Greenfield PM, Hernandez LM et Dapretto M (2018) "Peer Influence Via Instagram: Effects on Brain and Behavior in Adolescence and Young Adulthood". *Child development* 89(1): 37-47. DOI : 10.1111/cdev.12838.

Tufekci Z (2015) Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency. *Colorado Technology Law Journal* 13(2): 203.

Zuboff S L'Âge du capitalisme de surveillance. *2019*.

10 | Sitographie

https://www.cnil.fr/fr consulté le 3 Mai 2025

https://commission.europa.eu/index_fr consulté le 27 Avril 2025

https://www.oecd.org/fr.html consulté le 3 Mai 2025

https://www.ibm.com/fr-fr consulté le 28 Avril 2025

https://privacyinternational.org/fr consulté le 25 Avril 2025

https://www.ftc.gov/ consulté le 4 Mai 2025

https://solidproject.org/ consulté le 4 Mai 2025