



Vers de nouveaux modèles de partage de la connaissance

Manuel MUNIER

Université de Pau et des Pays de l'Adour, E2S UPPA

LIUPPA, Mont-de-Marsan, France

Laboratoire d'Informatique de l'Université de Pau et des Pays de l'Adour

*Équipe **ISI-Know***

(Ingénierie et Sécurité de l'Information par la gestion des connaissances)

Introduction

- **Thème É-EGC 2026 : l'IA dans la Cybersécurité : risque ou opportunité ?**
 - ce titre peut être interprété dans les 2 sens
 - ▷ utilisation des techniques d'IA pour « augmenter » les techniques de cybersécurité
 - ▷ assurer la cybersécurité des techniques d'IA

Introduction

- **Thème É-EGC 2026 : l'IA dans la Cybersécurité : risque ou opportunité ?**
 - ce titre peut être interprété dans les 2 sens
 - ▷ utilisation des techniques d'IA pour « augmenter » les techniques de cybersécurité
 - ▷ assurer la cybersécurité des techniques d'IA
 - un point essentiel dans ce domaine : le partage des connaissances
 - ▷ autant pour « alimenter » les IA de la cybersécurité
 - ▷ que pour (cyber)sécuriser les IA

Introduction

● Thème É-EGC 2026 : l'IA dans la Cybersécurité : risque ou opportunité ?

- ce titre peut être interprété dans les 2 sens
 - ▷ utilisation des techniques d'IA pour « augmenter » les techniques de cybersécurité
 - ▷ assurer la cybersécurité des techniques d'IA

- un point essentiel dans ce domaine : le partage des connaissances
 - ▷ autant pour « alimenter » les IA de la cybersécurité
 - ▷ que pour (cyber)sécuriser les IA

- objectif de cette présentation : vous sensibiliser aux enjeux liés au partage de données
 - ▷ avec une approche holistique : numérique, juridique, économique, sociale
 - ▷ avec un focus sur les thématiques d'EGC

Plan

- Mon parcours
- La problématique du partage de données
- La gestion des risques
- Les législations
- Les communs
- Encore des défis
- Conclusion

Ma trajectoire

- **Finalement... toujours guidée par la « sécurité »**

- DEA → logiques d'ordre supérieur, construction de preuves
- Thèse → systèmes transactionnels étendus (BdD), CSCW (Computer Supported Collaborative Work)
- PostDoc → mécanismes de négociation (~ « protocole »)

Ma trajectoire

● Finalement... toujours guidée par la « sécurité »

- DEA → logiques d'ordre supérieur, construction de preuves
- Thèse → systèmes transactionnels étendus (BdD), CSCW (Computer Supported Collaborative Work)
- PostDoc → mécanismes de négociation (~ « protocole »)
- Contrôle d'accès, contrôle d'usage
 - ▷ ≠ organisations → politiques/règles différentes, interopérabilité
 - ▷ → SSI (Sécurité des Systèmes d'Information)
- Contrôle d'usage → métadonnées
 - ▷ règles de sécurité dynamiques (contextuelles)
 - ▷ contrôle des actions → contrôle des utilisateurs, actions interdites, etc. → aspects juridiques

Ma trajectoire

● Finalement... toujours guidée par la « sécurité »

- Systèmes centralisés vs systèmes distribués
 - ▷ échanges de données, partage d'information
 - ▷ nouveaux usages → nouvelles vulnérabilités, nouveaux « risques »
 - ▷ ➔ gestion des risques liés à la sécurité de l'information (ex : EBIOS, ISO 27005)
 - ▷ ➔ nouveaux défis pour la sécurité → maîtrise du SI, qualité des données, etc.

Ma trajectoire

● Finalement... toujours guidée par la « sécurité »

- Systèmes centralisés vs systèmes distribués
 - ▷ échanges de données, partage d'information
 - ▷ nouveaux usages → nouvelles vulnérabilités, nouveaux « risques »
 - ▷ ➔ gestion des risques liés à la sécurité de l'information (ex : EBIOS, ISO 27005)
 - ▷ ➔ nouveaux défis pour la sécurité → maîtrise du SI, qualité des données, etc.
- Responsabilités dans le partage de données ?
 - ▷ cadre juridique, nouvelles réglementations
 - ▷ notion de gouvernance des données
- « Idéologie » du partage de l'information
 - ▷ évolution des modèles économiques autour de la donnée

Problématique

● Explosion du partage de données

- XXI^{ème} siècle = « société de l'information »
- Les NTIC génèrent des quantités de données qui ne cessent de croître
 - ▷ IoT, *smart cities*, industrie 4.0, jumeaux numériques,...
 - ▷ interconnexion des SI, systèmes de systèmes, *cloud*, *edge*,...
 - ▷ ➔ nouveaux services : transport, énergie, gestion des déchets, circulation, agriculture,...
 - ▷ ➔ nouveaux risques au regard de la sécurité de l'information

Problématique

● Explosion du partage de données

- XXI^{ème} siècle = « société de l'information »
- Les NTIC génèrent des quantités de données qui ne cessent de croître
 - ▷ IoT, *smart cities*, industrie 4.0, jumeaux numériques,...
 - ▷ interconnexion des SI, systèmes de systèmes, *cloud*, *edge*,...
 - ▷ ➔ nouveaux services : transport, énergie, gestion des déchets, circulation, agriculture,...
 - ▷ ➔ nouveaux risques au regard de la sécurité de l'information
- Extraction et Gestion des Connaissances (EGC 😊)
 - ▷ fouille de données, apprentissage, représentation, ontologies, métadonnées,...
 - ▷ acquisition, nettoyage, filtrage, stockage, requêtes,...
 - ▷ données FAIR (*Findable, Accessible, Interoperable, Reusable*), science ouverte, intelligence,...
 - ▷ ➔ données exploitées 📈, données générées 📈

Problématique

● « La véritable richesse de la connaissance ne réside pas dans sa possession, mais dans sa diffusion »

- Mais comment partager ces données / connaissances ?
 - ▷ technique ✓ → télécoms, crypto, blockchain, *data stores*, contrôle d'accès, traçabilité (?),...
 - ▷ stratégie ✗ → règles ? enjeux ?... ➔ responsabilités, gouvernance des données, etc.

Problématique

● « La véritable richesse de la connaissance ne réside pas dans sa possession, mais dans sa diffusion »

- Mais comment partager ces données / connaissances ?
 - ▷ technique ✓ → télécoms, crypto, blockchain, *data stores*, contrôle d'accès, traçabilité (?),...
 - ▷ stratégie ✗ → règles ? enjeux ?... → responsabilités, gouvernance des données, etc.
- Ce qu'il manque
 - ▷ garder le contrôle sur les données que nous partageons → les utilisateurs ont besoin de confiance et de transparence
 - ▷ ne pas imposer un outil unique et trop strict
 - ▷ **découplage producteur / consommateur** → ils ne se connaissent pas nécessairement l'un l'autre

Problématique

● Vision réaliste ?

- **numérique** ➔ modèle, web sémantique, raisonnement
 - ▷ gestion des risques ➔ CID + traçabilité (ex : provenance) + qualité (ex : confiance, authenticité), nouvelles vulnérabilités spécifiques (ex : sur les jeux de données)
 - ▷ politique de sécurité (contrôle d'usage), licences, architecture distribuée, etc.
 - ▷ ingénierie des connaissances, intelligence informationnelle, etc. ➔ EGC

Problématique

● Vision réaliste ?

- **numérique** → modèle, web sémantique, raisonnement
 - ▷ gestion des risques → CID + traçabilité (ex : provenance) + qualité (ex : confiance, authenticité), nouvelles vulnérabilités spécifiques (ex : sur les jeux de données)
 - ▷ politique de sécurité (contrôle d'usage), licences, architecture distribuée, etc.
 - ▷ ingénierie des connaissances, intelligence informationnelle, etc. → EGC
- **droit** → publication récente de nouveaux textes (FR & EU)
 - ▷ importance de la donnée, confiance, souveraineté, etc. → stratégie, géo-politique

Problématique

● Vision réaliste ?

- **numérique** → modèle, web sémantique, raisonnement
 - ▷ gestion des risques → CID + traçabilité (ex : provenance) + qualité (ex : confiance, authenticité), nouvelles vulnérabilités spécifiques (ex : sur les jeux de données)
 - ▷ politique de sécurité (contrôle d'usage), licences, architecture distribuée, etc.
 - ▷ ingénierie des connaissances, intelligence informationnelle, etc. → EGC
- **droit** → publication récente de nouveaux textes (FR & EU)
 - ▷ importance de la donnée, confiance, souveraineté, etc. → stratégie, géo-politique
- **socio-économie** → évolution des priorités, « prise de conscience »
 - ▷ qualité des données, valeur d'usage prime sur propriété, gestion par les Communs

Gestion des risques

● ISO 27005, EBIOS, etc.

- définit une démarche structurée et itérative de gestion des risques liés à la sécurité de l'information, centrée sur la protection des actifs informationnels (ex : confidentialité, intégrité, disponibilité)
- préconise d'identifier, analyser, évaluer puis traiter les risques de sécurité (scénarios), en s'appuyant sur une tolérance au risque définie par l'organisation et alignée sur ses **objectifs** business
- grandes étapes :
 - ▷ établir le contexte et le périmètre (actifs, menaces, contraintes, parties prenantes)
 - ▷ identifier les risques, puis les analyser (probabilité et **impact**) et les évaluer par rapport à des **critères** prédéfinis
 - ▷ choisir des traitements (atténuation, évitement, transfert, acceptation) et mettre en œuvre des contrôles, avec un suivi et une revue réguliers
- approche proactive, documentée et reproductible ➡ « audit »

Lois & Règlements

● Loi pour une République Numérique (LRN)

- loi française – 7 octobre **2016** → concilier transparence administrative et protection de la vie privée
 - ▷ introduit l'**Open Data** « par principe »
 - depuis le 7 octobre 2018, les collectivités de plus de 3 500 habitants et les administrations de plus de 50 agents doivent publier en ligne leurs bases de données et les données présentant un intérêt économique, social, sanitaire ou environnemental
 - ▷ les documents comportant des données nominatives ne portant pas atteinte à la vie privée peuvent être publiés sans anonymisation préalable

Lois & Règlements

● Loi pour une République Numérique (LRN)

- loi française – 7 octobre **2016** → concilier transparence administrative et protection de la vie privée
 - ▷ introduit l'**Open Data** « par principe »
 - depuis le 7 octobre 2018, les collectivités de plus de 3 500 habitants et les administrations de plus de 50 agents doivent publier en ligne leurs bases de données et les données présentant un intérêt économique, social, sanitaire ou environnemental
 - ▷ les documents comportant des données nominatives ne portant pas atteinte à la vie privée peuvent être publiés sans anonymisation préalable
 - ▷ l'ouverture des données concerne aussi les algorithmes publics, de plus en plus fréquents dans les décisions administratives (par exemple pour le calcul de l'impôt ou l'affectation des élèves dans les établissements scolaires ou l'enseignement supérieur)
 - toute personne destinataire d'une décision fondée sur un traitement algorithmique peut à présent demander à l'administration les règles définissant ce traitement et ses principales caractéristiques (sauf exceptions)
- nouvelle mission de l'État : service public de la donnée → mission Etalab (data.gouv.fr) → ALLiance

Lois & Règlements

● Règlement Général sur la Protection des Données (RGPD)

- Union Européenne – 25 mai **2018**
 - ▷ données personnelles uniquement ; principes, droits, obligations ; guides
 - « toute information se rapportant à une personne physique identifiée ou identifiable »
 - **directement** (ex : nom, prénom)
 - **indirectement** (ex : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique,...)
 - ▷ l'identification d'une personne physique peut être réalisée :
 - à partir d'**une seule donnée** (ex : numéro de sécurité sociale, ADN)
 - à partir du **croisement d'un ensemble de données** (ex : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)
- ex : base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y-compris si leur nom n'est pas stocké → traitement de données personnelles
 - ▷ le 30 décembre 2025, la CNIL a prononcé une sanction administrative de 3,5 millions d'euros à l'encontre d'une société ayant transmis les données de ses clients fidèles à un réseau social (🌐)

Lois & Règlements

● Data Governance Act (DGA)

- Union Européenne – 23 juin 2022 – applicable depuis septembre **2023**
 - ▷ issu de la stratégie européenne pour les données (2020)
 - ▷ objectifs :
 - faciliter la **libre circulation** et le **partage volontaire** des données entre entreprises, administrations publiques et particuliers au sein du marché intérieur européen, tout en assurant une protection rigoureuse des droits fondamentaux et des valeurs européennes, notamment en matière de protection des données personnelles
 - renforcer la confiance dans les services de partage de données en établissant des normes strictes pour les fournisseurs de ces services → garantir le respect des exigences de confidentialité et de sécurité
 - introduction du concept d'**altruisme en matière de données** → encourager les particuliers et les organisations à partager volontairement leurs données à des fins d'intérêt général (ex : la recherche scientifique, la santé publique, ou encore la lutte contre le changement climatique)
 - ▷ *common data-sharing spaces* → **data holders, data users, data intermediaries**
 - ▷ concerne aussi bien les **données personnelles** et que les **données non personnelles**

Lois & Règlements

● Data Act

- Union Européenne – 11 janvier **2024** – applicable depuis septembre **2025**
 - ▷ objectif :
 - exploiter le potentiel de la quantité de données (industrielles) ; en faire bénéficier l'économie et la société
 - ▷ s'applique à toutes les **données produites** par l'utilisation d'objets connectés et les **services** qui leur sont associés, qu'elles soient personnelles ou non
 - les **objets concernés** sont tous ceux qui communiquent des données par le biais d'Internet ou un autre réseau public
 - ▷ ex : véhicule connecté, montre ou bracelet de santé connecté, thermostat intelligent, machine industrielle équipée de capteurs, etc.
 - les **services associés** sont ceux nécessaires au fonctionnement de ces objets
 - ▷ ex : application mobile qui permet de régler un thermostat connecté, plateforme en ligne où sont affichées les données d'un capteur, service de gestion commerciale de flotte de véhicules, lié au boîtier télématique installé dans les véhicules, assistant intelligent intégré au produit, etc.

Lois & Règlements

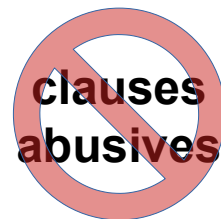
● Data Act (suite)

- Union Européenne – 11 janvier **2024** – applicable depuis septembre **2025**
 - ▷ portée :
 - organismes du secteur public, institutions, agences ou organes de l'Union européenne
 - ▷ dans certains cas, ces organismes peuvent exiger l'accès à certaines données afin de répondre à des situations urgentes ou à des missions d'intérêt public
 - fournisseurs de services de traitement de données (ex : un service d'informatique en nuage) proposés dans l'Union européenne
 - participants aux espaces de données et vendeurs d'applications utilisant des contrats intelligents, c'est-à-dire des acteurs qui conçoivent ou utilisent des contrats automatisés dans leurs services

Lois & Règlements

● Data Act (suite)

- Union Européenne – 11 janvier **2024** – applicable depuis septembre **2025**
 - ▷ portée :
 - organismes du secteur public, institutions, agences ou organes de l'Union européenne
 - ▷ dans certains cas, ces organismes peuvent exiger l'accès à certaines données afin de répondre à des situations urgentes ou à des missions d'intérêt public
 - fournisseurs de services de traitement de données (ex : un service d'informatique en nuage) proposés dans l'Union européenne
 - participants aux espaces de données et vendeurs d'applications utilisant des contrats intelligents, c'est-à-dire des acteurs qui conçoivent ou utilisent des contrats automatisés dans leurs services
 - ▷ obligations :
 - rendre les données accessibles aux utilisateurs dès la conception
 - mettre les données à disposition de l'utilisateur sur demande
 - permettre le partage des données à des tiers (sur demande de l'utilisateur)
 - garantir la transparence sur les données générées par les objets connectés
 - faciliter le changement de prestataires de services d'informatique en nuage (*cloud*)



Lois & Règlements

● Artificial Intelligence Act (AI Act)

- Union Européenne – 12 juillet **2024**
 - ▷ vise à réguler des produits d'intelligence artificielle qui sont commercialisés sur le marché européen
 - ▷ **approche « par les risques »** → il ne s'agit pas de classer les IA qui seront autorisées et celles qui seront interdites en fonction de la technologie sous-jacente, mais en fonction de l'usage prévu de la technologie
 - les différents niveaux de risque entraîneront une réglementation plus ou moins stricte

Lois & Règlements

● Artificial Intelligence Act (AI Act)

- Union Européenne – 12 juillet **2024**
 - ▷ vise à réguler des produits d'intelligence artificielle qui sont commercialisés sur le marché européen
 - ▷ **approche « par les risques »** → il ne s'agit pas de classer les IA qui seront autorisées et celles qui seront interdites en fonction de la technologie sous-jacente, mais en fonction de l'usage prévu de la technologie
 - les différents niveaux de risque entraîneront une réglementation plus ou moins stricte
 - ▷ exigences en matière de **transparence** :
 - divulguer que le contenu a été généré par l'IA
 - concevoir le modèle de manière à empêcher la génération de contenus illégaux
 - publier des résumés des données protégées par le droit d'auteur utilisées pour la formation

Lois & Règlements

● Artificial Intelligence Act (AI Act)

- Union Européenne – 12 juillet **2024**
 - ▷ vise à réguler des produits d'intelligence artificielle qui sont commercialisés sur le marché européen
 - ▷ **approche « par les risques »** → il ne s'agit pas de classer les IA qui seront autorisées et celles qui seront interdites en fonction de la technologie sous-jacente, mais en fonction de l'usage prévu de la technologie
 - les différents niveaux de risque entraîneront une réglementation plus ou moins stricte
 - ▷ exigences en matière de **transparence** :
 - divulguer que le contenu a été généré par l'IA
 - concevoir le modèle de manière à empêcher la génération de contenus illégaux
 - publier des résumés des données protégées par le droit d'auteur utilisées pour la formation
 - ▷ mais également
 - exigences d'évaluation et de tests adversariaux, d'atténuation des risques, de déclaration des incidents sérieux, de cybersécurité et d'analyse de la consommation d'énergie

Lois & Règlements

● Digital Services Act (DSA)

- Union Européenne – applicable depuis le 17 février **2024**
 - ▷ fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux
 - attaques racistes, images pédopornographiques, désinformation, vente de drogues ou de contrefaçons, etc.
 - ▷ succède à la directive dite e-commerce du 8 juin 2000, devenue dépassée

Lois & Règlements

● Digital Services Act (DSA)

- Union Européenne – applicable depuis le 17 février **2024**
 - ▷ fixe un ensemble de règles pour responsabiliser les plateformes numériques et lutter contre la diffusion de contenus illicites ou préjudiciables ou de produits illégaux
 - ➔ attaques racistes, images pédopornographiques, désinformation, vente de drogues ou de contrefaçons, etc.
 - ▷ succède à la directive dite e-commerce du 8 juin 2000, devenue dépassée
 - ▷ mais également ➔ **transparence en ligne**
 - ➔ les plateformes doivent rendre plus transparentes leurs décisions en matière de modération des contenus
 - ➔ les plateformes ont l'obligation d'expliquer le fonctionnement des algorithmes qu'elles utilisent pour recommander certains contenus publicitaires en fonction du profil des utilisateurs
 - ➔ la publicité ciblée pour les mineurs est désormais interdite pour toutes les plateformes (idem pour la publicité basée sur des données sensibles comme les opinions politiques, la religion ou l'orientation sexuelle)
- ▷ atténuation des risques et réponse aux crises ➔ gestion des risques

Et donc ?

- L'Europe et ses citoyens prennent conscience de la valeur de la donnée

- la donnée (ou l'information) est une richesse qu'il faut protéger
- la donnée ne doit pas devenir la propriété d'acteurs privés (qui facturent des droits d'accès)
- le partage doit être encouragé, tout en veillant aux **responsabilités** des acteurs ➔ **confiance**

Et donc ?

● L'Europe et ses citoyens prennent conscience de la valeur de la donnée

- la donnée (ou l'information) est une richesse qu'il faut protéger
- la donnée ne doit pas devenir la propriété d'acteurs privés (qui facturent des droits d'accès)
- le partage doit être encouragé, tout en veillant aux **responsabilités** des acteurs → **confiance**

● Une autre approche du partage de l'information

- découplage producteur / consommateur → ils ne se connaissent pas nécessairement l'un l'autre
- pas d'autorité centrale pour le contrôle du partage → les acteurs se regroupent en communautés
- gouvernance des données
 - ▷ règles de contrôle d'usage fixées par celui qui partage → **autodétermination informationnelle**
 - ▷ métadonnées pour améliorer la **qualité des données** et la **responsabilité**

Communs

● En bref...

- modèle de gestion des données proposé par l'économiste Elinor Ostrom (1977, 1990), Prix Nobel d'économie en 2009
- « *a new economic paradigm that prioritizes **use value over ownership*** » (Jeremy Rifkin, 2014)
- Communs informationnels : « *resources governed by a system of **distributed rights** and a **governance structure** that ensures compliance with rights and obligations* » (Benjamin Coriat, 2015)

Communs

● En bref...

- modèle de gestion des données proposé par l'économiste Elinor Ostrom (1977, 1990), Prix Nobel d'économie en 2009
- « *a new economic paradigm that prioritizes **use value over ownership*** » (Jeremy Rifkin, 2014)
- Communs informationnels : « *resources governed by a system of **distributed rights** and a **governance structure** that ensures compliance with rights and obligations* » (Benjamin Coriat, 2015)

● Définition Wikipédia

- Les **communs** sont des ressources partagées, gérées et maintenues collectivement par une communauté ; celle-ci établit des règles dans le but de préserver et pérenniser ces ressources tout en fournissant aux membres de cette communauté la possibilité et le droit de les utiliser, voire, si la communauté le décide, en octroyant ce droit à tous. Ces ressources peuvent être naturelles (une forêt, une rivière), matérielles (une machine-outil, une maison, une centrale électrique) ou immatérielles (une connaissance, un logiciel).

Communs

● Histoire d'une idée

- l'idée de biens communs n'est pas nouvelle, on peut même retrouver celle-ci dès l'Antiquité romaine dans le Code de Justinien daté du VI^{ème} siècle
 - ▷ en droit romain existait la distinction entre les biens privés (Res Privatae), les biens publics (Res Publicae), les choses n'appartenant à personne (Res Nullius) et les "choses communes" (Res Communis), qui étaient notamment les rivières, les côtes, etc.

Communs

● Histoire d'une idée

- l'idée de biens communs n'est pas nouvelle, on peut même retrouver celle-ci dès l'Antiquité romaine dans le Code de Justinien daté du VI^{ème} siècle
 - ▷ en droit romain existait la distinction entre les biens privés (Res Privatae), les biens publics (Res Publicae), les choses n'appartenant à personne (Res Nullius) et les "choses communes" (Res Communis), qui étaient notamment les rivières, les côtes, etc.
- ⋮
- c'est en 1990 dans « *La Gouvernance des biens communs : pour une nouvelle approche des ressources naturelles* » d'**Elinor Ostrom** (économiste, politologue et Prix Nobel d'économie américaine) que cette idée connaît un regain d'intérêt et une nouvelle perception
 - ▷ dans cet ouvrage, la chercheuse étudie la gestion de ressources naturelles par des groupes qui utilisent des formes de propriété collective nommées « **biens communs** »
 - ▷ l'histoire et le monde contemporain étant beaucoup perçus au travers de la privatisation ou de la gestion par l'État, cette analyse démontre qu'ont existé des régimes de propriété collective pérennes

Communs

● Communs numériques

➤ définition

- ▷ un commun numérique est une ressource numérique produite, gérée et gouvernée par une communauté d'utilisateurs selon des règles de gouvernance conjointement élaborées ; la dématérialisation de la ressource et les licences libres associées permettent à un commun numérique d'offrir à tous les membres de sa communauté les libertés d'accès, d'usage, d'étude, d'amélioration et de partage de la ressource
- ▷ parmi les exemples les plus cités, on retrouve l'encyclopédie [Wikipédia](#), le projet [OpenStreetMap](#) de cartographie en ligne, le projet [Open Food Facts](#), base des données nutritionnelles et de nombreux logiciels libres tels que [VLC](#) ou le système d'exploitation GNU/ [Linux](#)

Communs

● Communs numériques

➤ définition

- ▷ un commun numérique est une ressource numérique produite, gérée et gouvernée par une communauté d'utilisateurs selon des règles de gouvernance conjointement élaborées ; la dématérialisation de la ressource et les licences libres associées permettent à un commun numérique d'offrir à tous les membres de sa communauté les libertés d'accès, d'usage, d'étude, d'amélioration et de partage de la ressource
- ▷ parmi les exemples les plus cités, on retrouve l'encyclopédie [Wikipédia](#), le projet [OpenStreetMap](#) de cartographie en ligne, le projet [Open Food Facts](#), base des données nutritionnelles et de nombreux logiciels libres tels que [VLC](#) ou le système d'exploitation GNU/ [Linux](#)

➤ nouvelles caractéristiques des communs numériques

- ▷ l'usage de la ressource par les uns ne limite pas les possibilités d'usage par les autres (**la ressource est non rivale**)
- ▷ sa préservation ne passe pas par la réservation du droit d'usage à une communauté restreinte (**la ressource est non-exclusive**)
- ➔ les communs numériques gagnent à être partagés, car ce partage augmente directement la valeur d'usage de la ressource et permet par ailleurs d'étendre la communauté qui la préservera

Communs

● Intérêt des communs numériques

➤ horizontalité

- ▷ là où l'action des États, voire des collectivités est généralement très verticale (c'est-à-dire qu'elle s'impose d'un décideur aux citoyens), les communs sont au contraire horizontaux et basés sur la participation volontaire de celles et ceux qui vont l'enrichir
- ▷ l'Open et les communs sont deux faces d'une même volonté de participation et de partage libre en dehors du contrôle, qu'il soit public ou privé
- ▷ il y a un fonctionnement vertueux de la participation qui enrichit la ressource : plus celle-ci est de qualité par l'action de tous, plus celle-ci est attractive et donc attire plus de participants
- ▷ cette horizontalité se double d'une vigilance concernant à la fois les participations et la **gouvernance** de la ressource

Communs

● Intérêt des communs numériques

➤ opposition aux stratégies des GAFAM ou des États

- ▷ si l'internet « des origines » était perçu comme un commun par celles et ceux qui l'ont pensé et conçu, il est devenu de plus en plus privatisé, notamment par les GAFAM qui ont à la fois capté les usages et imposé un enfermement, notamment dans le cadre des réseaux sociaux
- ▷ ne plus quitter le réseau social en mobilisant en permanence l'attention, est l'économie qui est à la base des plateformes
- ▷ en proposant des alternatives (OpenStreetMap par rapport à Google Maps par exemple), les communs luttent contre la captation des données personnelles par ces entreprises
- ▷ certains gouvernements, en imposant un contrôle strict de ce qui peut exister sur le réseau national, enferment eux aussi leurs citoyens

➔ au-delà de ce partage, de cette ouverture et de cette exigence **les communs ont donc aussi un rôle politique** ; ils permettent une réappropriation de ses données, un meilleur contrôle de ses usages

Défis pour le partage de la connaissance

- **Gouvernance des données**

- transparence et traçabilité
 - ▷ la gouvernance des données requiert une visibilité des flux et une clarté des règles d'usage
 - ▷ protéger les communs numériques contre la « contamination » des données → entretien collectif permanent

Défis pour le partage de la connaissance

● Gouvernance des données

- transparence et traçabilité
 - ▷ la gouvernance des données requiert une visibilité des flux et une clarté des règles d'usage
 - ▷ protéger les communs numériques contre la « contamination » des données → entretien collectif permanent
- incitations douces et réciprocité
 - ▷ proposer des incitations non coercitives (incitations comportementales, reconnaissance académique et simplification des démarches) → « **nudges** »
 - ▷ la confiance et la communication, comme l'a montré Ostrom (2010), favorisent la coopération

Défis pour le partage de la connaissance

● Gouvernance des données

- transparence et traçabilité
 - ▷ la gouvernance des données requiert une visibilité des flux et une clarté des règles d'usage
 - ▷ protéger les communs numériques contre la « contamination » des données → entretien collectif permanent
- incitations douces et réciprocité
 - ▷ proposer des incitations non coercitives (incitations comportementales, reconnaissance académique et simplification des démarches) → « **nudges** »
 - ▷ la confiance et la communication, comme l'a montré Ostrom (2010), favorisent la coopération
- gouvernance distribuée et subsidiarité
 - ▷ une toile sans centre, une gouvernance polycentrique
 - ▷ espaces de décision distribués (laboratoires, communautés, agences), dotés de règles communes, mais adaptables aux contextes, et pour lesquels la subsidiarité devient un principe de durabilité

Défis pour le partage de la connaissance

● Gouvernance des données

- interopérabilité et diplomatie normative
 - ▷ construction de normes ouvertes et interopérables dans la gouvernance des données
 - ▷ attention à l'« effet Bruxelles » ! (Bradford, 2012, 2020)

Défis pour le partage de la connaissance

● Gouvernance des données

- interopérabilité et diplomatie normative
 - ▷ construction de normes ouvertes et interopérables dans la gouvernance des données
 - ▷ attention à l'« effet Bruxelles » ! (Bradford, 2012, 2020)
- résilience et adaptation évolutive
 - ▷ intégrer des mécanismes de rétroaction pour s'adapter aux crises, aux tensions géopolitiques ou aux évolutions technologiques (Obendiek, 2023)
 - ▷ ex : règles évolutives et participatives

Conclusion

● Vers de meilleures pratiques d'échange

- le partage d'information peut être une source de nouvelles vulnérabilités → nouveaux risques
- si nous voulons que les utilisateurs partagent davantage, nous devons leur fournir des outils de confiance et de responsabilité → **gouvernance des données**, gestion par les **Communs**

Conclusion

● Vers de meilleures pratiques d'échange

- le partage d'information peut être une source de nouvelles vulnérabilités → nouveaux risques
- si nous voulons que les utilisateurs partagent davantage, nous devons leur fournir des outils de confiance et de responsabilité → **gouvernance des données**, gestion par les **Communs**
- approche holistique
 - économie, théorie de communs
 - analyse comportementale du droit
 - diplomatie numérique et géopolitique de la connaissance

Conclusion

● Vers de meilleures pratiques d'échange

- le partage d'information peut être une source de nouvelles vulnérabilités → nouveaux risques
- si nous voulons que les utilisateurs partagent davantage, nous devons leur fournir des outils de confiance et de responsabilité → **gouvernance des données**, gestion par les **Communs**
- approche holistique
 - économie, théorie de communs
 - analyse comportementale du droit
 - diplomatie numérique et géopolitique de la connaissance
- ingénierie des connaissances & IA pour la cybersécurité, mais aussi cybersécurité pour l'IC et l'IA

Conclusion

● Vers de meilleures pratiques d'échange

- le partage d'information peut être une source de nouvelles vulnérabilités → nouveaux risques
- si nous voulons que les utilisateurs partagent davantage, nous devons leur fournir des outils de confiance et de responsabilité → **gouvernance des données**, gestion par les **Communs**
- approche holistique
 - économie, théorie de communs
 - analyse comportementale du droit
 - diplomatie numérique et géopolitique de la connaissance
- ingénierie des connaissances & IA pour la cybersécurité, mais aussi cybersécurité pour l'IC et l'IA
- partager « mieux » pour partager « moins » ? → **minimisation des données, numérique responsable**

Merci de votre attention

CONTACT

Manuel MUNIER

Université de Pau et des Pays de l'Adour, E2S UPPA
LIUPPA, Mont-de-Marsan, France

Équipe *ISI-Know*

(Ingénierie et Sécurité de l'Information par la gestion des connaissances)

Manuel.Munier@univ-pau.fr
<http://munier.perso.univ-pau.fr/>

